日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　６月２８日

出願番号
Application Number: 特願２００２－１８９０７２

[ST.10/C]: [ＪＰ２００２－１８９０７２]

出願人
Applicant(s): インクリメント・ピー株式会社

２００３年　２月　７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００５７８３

【書類名】　特許願
【整理番号】　57P0010
【提出日】　平成14年 6月28日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　東京都目黒区下目黒１丁目７番１号　インクリメント・ピー株式会社内
　【氏名】　柴田　紀正
【特許出願人】
　【識別番号】　595105515
　【氏名又は名称】　インクリメント・ピー株式会社
【代理人】
　【識別番号】　100083839
　【弁理士】
　【氏名又は名称】　石川　泰男
　【電話番号】　03-5443-8461
【手数料の表示】
　【予納台帳番号】　007191
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9814643
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体

【特許請求の範囲】

【請求項１】　通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムであって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証手段と、

前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証手段と、

前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、

を備えたことを特徴とする通信機器認証システム。

【請求項２】　請求項１に記載の通信機器認証システムにおいて、

前記第１のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第２のキー情報がセッションキーであることを特徴とする通信機器認証システム。

【請求項３】　請求項１または２に記載の通信機器認証システムにおいて、

前記第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証システム。

【請求項４】　請求項１に記載の通信機器認証システムにおいて、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたこ

とを特徴とする通信機器認証システム。

【請求項５】　請求項１に記載の通信機器認証システムにおいて、

前記サーバ装置により生成された第２のキー情報を認証する第３の認証手段を、前記サーバ装置とは別のサーバ装置に設けたことを特徴とする通信機器認証システム。

【請求項６】　請求項１または５に記載の通信機器認証システムにおいて、

前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証システム。

【請求項７】　通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証方法であって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証工程と、

前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証工程と、

前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程と、

を備えたことを特徴とする通信機器認証方法。

【請求項８】　請求項７に記載の通信機器認証方法において、

前記第１のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第２のキー情報がセッションキーであることを特徴とする通信機器認証方法。

【請求項９】　請求項７または８に記載の通信機器認証システムにおいて、

前記第１の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアク

セスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証方法。

【請求項１０】　請求項７に記載の通信機器認証方法において、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする通信機器認証方法。

【請求項１１】　請求項７に記載の通信機器認証方法において、

前記サーバ装置により生成された第２のキー情報を認証する第３の認証工程を、前記サーバ装置とは別のサーバ装置にて実行することを特徴とする通信機器認証方法。

【請求項１２】　請求項７または１１に記載の通信機器認証方法において、

前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証方法。

【請求項１３】　通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいて前記通信端末装置にデータを供給する通信機器認証サーバ装置であって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記通信端末装置に送信する第１の認証手段と、

前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記通信端末装置に送信する第２の認証手段と、

前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、

を備えたことを特徴とする通信機器認証サーバ装置。

【請求項１４】　請求項１３に記載の通信機器認証サーバ装置において、

前記第１のキー情報がアクセスされるアクセスキーであって、前記第２のキー

情報がセッションキーであることを特徴とする通信機器認証サーバ装置。

【請求項１５】　請求項１３または１４に記載の通信機器認証サーバ装置において、

前記第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証サーバ装置。

【請求項１６】　請求項１３に記載の通信機器認証サーバ装置において、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに受信可能としたことを特徴とする通信機器認証サーバ装置。

【請求項１７】　請求項１３に記載の通信機器認証サーバ装置において、

前記生成された第２のキー情報を認証する第３の認証手段を、別のサーバ装置に設けたことを特徴とする通信機器認証サーバ装置。

【請求項１８】　請求項１３または１７に記載の通信機器認証サーバ装置において、

前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証サーバ装置。

【請求項１９】　通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムに含まれるコンピュータを、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証手段、

前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証手段、

前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段、

として機能させることを特徴とする通信機器認証用プログラム。

【請求項２０】　請求項１９に記載の通信機器認証用プログラムにおいて、

前記第１のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第２のキー情報がセッションキーであるように機能させることを特徴とする通信機器認証用プログラム。

【請求項２１】　請求項１９または２０に記載の通信機器認証用プログラムにおいて、

前記第１の認証手段として機能するコンピュータを、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与するように機能させることを特徴とする通信機器認証用プログラム。

【請求項２２】　請求項１９に記載の通信機器認証用プログラムにおいて、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能とするように機能させることを特徴とする通信機器認証用プログラム。

【請求項２３】　請求項１９に記載の通信機器認証用プログラムにおいて、

前記サーバ装置により生成された第２のキー情報を認証する第３の認証手段として機能するコンピュータを、前記サーバ装置とは別のサーバ装置に機能させることを特徴とする通信機器認証用プログラム。

【請求項２４】　請求項１９または２３に記載の通信機器認証用プログラムにおいて、

前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定するように機能させることを特徴とする通信機器認証用プログラム。

【請求項２５】　請求項１９乃至２４のいずれか一項に記載の通信機器認証用プログラムが記録されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体に係り、特に通信カーナビゲーション装置、携帯情報端末などの通信端末装置で通信を行う際にセキュリティを確保した通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体の技術分野に関する。

【０００２】

【従来の技術】

一般に、パーソナルコンピュータ（以下、パソコンと略称する。）などの通信端末装置における認証方式は、フォームによって転送される文書を暗号化する技術を備えたＳＳＬ（Ｓｅｃｕｒｉｔｙ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）に対応した通信端末装置からインターネットなどの通信手段を介して入力されるパスワードなどのユーザ特定情報に基づいて通信端末装置を使用するユーザに対してサーバ装置が認証を行い、その認証結果に基づいてサーバ装置から上記通信端末装置に各種データを供給可能な方式である。

【０００３】

【発明が解決しようとする課題】

しかしながら、上述した従来の認証方式では、ＳＳＬに対応した通信端末装置で認証を行っているため、セキュリティ上問題がないものの、ＣＰＵの容量が小さい通信端末装置や、ＳＳＬに対応することができない通信端末装置で認証を行う場合には、パスワードなどのユーザ特定情報が漏洩する可能性がある。そして、そのユーザ特定情報が漏洩すると、ユーザ以外の者に悪用されることがあり、ユーザにとって多大な被害を被る可能性がある。

【０００４】

本発明は、上記事情を考慮してなされたもので、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、不正アクセスを防止し、セキュリティを著しく向上させることのできる通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記

録媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記課題を解決するため、請求項１に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムであって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証手段と、前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証手段と、前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、を備えたことを特徴とする。

【０００６】

請求項１に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０００７】

上記課題を解決するため、請求項２に記載の発明は、請求項１に記載の通信機器認証システムにおいて、前記第１のキー情報が前記サーバ装置に対してアクセ

スするアクセスキーであって、前記第２のキー情報がセッションキーであることを特徴とする。

【０００８】

請求項２に記載の発明によれば、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０００９】

上記課題を解決するため、請求項３に記載の発明は、請求項１または２に記載の通信機器認証システムにおいて、前記第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

【００１０】

請求項３に記載の発明によれば、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【００１１】

上記課題を解決するため、請求項４に記載の発明は、請求項１に記載の通信機器認証システムにおいて、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする。

【００１２】

請求項４に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリ

ティを一段と高めることができる。

【００１３】

上記課題を解決するため、請求項５に記載の発明は、請求項１に記載の通信機器認証システムにおいて、前記サーバ装置により生成された第２のキー情報を認証する第３の認証手段を、前記サーバ装置とは別のサーバ装置に設けたことを特徴とする。

【００１４】

請求項５に記載の発明によれば、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【００１５】

上記課題を解決するため、請求項６に記載の発明は、請求項１または５に記載の通信機器認証システムにおいて、前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

【００１６】

請求項６に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【００１７】

上記課題を解決するため、請求項７に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証方法であって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証工程と、前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証工程と、前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内の

み許可するアクセス許可工程と、を備えたことを特徴とする。

【００１８】

請求項７に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証工程と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証工程と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【００１９】

上記課題を解決するため、請求項８に記載の発明は、請求項７に記載の通信機器認証方法において、前記第１のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第２のキー情報がセッションキーであることを特徴とする。

【００２０】

請求項８に記載の発明によれば、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【００２１】

上記課題を解決するため、請求項９に記載の発明は、請求項７または８に記載の通信機器認証方法において、前記第１の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

【００２２】

請求項９に記載の発明によれば、第１の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【００２３】

上記課題を解決するため、請求項１０に記載の発明は、請求項７に記載の通信機器認証方法において、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする。

【００２４】

請求項１０に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【００２５】

上記課題を解決するため、請求項１１に記載の発明は、請求項７に記載の通信機器認証方法において、前記サーバ装置により生成された第２のキー情報を認証する第３の認証工程を、前記サーバ装置とは別のサーバ装置にて実行することを特徴とする。

【００２６】

請求項１１に記載の発明によれば、第２のキー情報を認証する第３の認証工程を別のサーバ装置にて実行することにより、サーバ装置のＣＰＵ容量を低減させることができる。

【００２７】

上記課題を解決するため、請求項１２に記載の発明は、請求項７または１１に記載の通信機器認証方法において、前記別のサーバ装置は、前記第２のキー情報

を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

【００２８】

請求項１２に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【００２９】

上記課題を解決するため、請求項１３に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいて前記通信端末装置にデータを供給する通信機器認証サーバ装置であって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記通信端末装置に送信する第１の認証手段と、前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記通信端末装置に送信する第２の認証手段と、前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、を備えたことを特徴とする。

【００３０】

請求項１３に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成して通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【００３１】

上記課題を解決するため、請求項１４に記載の発明は、請求項１３に記載の通信機器認証サーバ装置において、前記第１のキー情報がアクセスされるアクセスキーであって、前記第２のキー情報がセッションキーであることを特徴とする。

【００３２】

請求項１４に記載の発明によれば、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【００３３】

上記課題を解決するため、請求項１５に記載の発明は、請求項１３または１４に記載の通信機器認証サーバ装置において、前記第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

【００３４】

請求項１５に記載の発明によれば、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【００３５】

上記課題を解決するため、請求項１６に記載の発明は、請求項１３に記載の通信機器認証サーバ装置において、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに受信可能としたことを特徴とする。

【００３６】

請求項１６に記載の発明によれば、通信端末装置に予め設定された装置識別情

報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【００３７】

上記課題を解決するため、請求項１７に記載の発明は、請求項１３に記載の通信機器認証サーバ装置において、前記生成された第２のキー情報を認証する第３の認証手段を、別のサーバ装置に設けたことを特徴とする。

【００３８】

請求項１７に記載の発明によれば、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【００３９】

上記課題を解決するため、請求項１８に記載の発明は、請求項１３または１７に記載の通信機器認証サーバ装置において、前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

【００４０】

請求項１８に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【００４１】

上記課題を解決するため、請求項１９に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムに含まれるコンピュータを、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第１の認証手段、前記通信端末装置から送信される前記第１のキー情報を認証し、当該第１のキー情報に基づいて前記データに対してアクセスする第２のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第２の認証手

段、前記通信端末装置から前記サーバ装置への前記第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることを特徴とする。

【００４２】

請求項１９に記載の発明によれば、コンピュータを、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証手段、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証手段、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【００４３】

上記課題を解決するため、請求項２０に記載の発明は、請求項１９に記載の通信機器認証用プログラムにおいて、前記第１のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第２のキー情報がセッションキーであるように機能させることを特徴とする。

【００４４】

請求項２０に記載の発明によれば、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【００４５】

上記課題を解決するため、請求項２１に記載の発明は、請求項１９または２０に記載の通信機器認証用プログラムにおいて、前記第１の認証手段として機能す

るコンピュータを、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与するように機能させることを特徴とする。

【００４６】

請求項２１に記載の発明によれば、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【００４７】

上記課題を解決するため、請求項２２に記載の発明は、請求項１９に記載の通信機器認証用プログラムにおいて、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能とするように機能させることを特徴とする。

【００４８】

請求項２２に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【００４９】

上記課題を解決するため、請求項２３に記載の発明は、請求項１９に記載の通信機器認証用プログラムにおいて、前記サーバ装置により生成された第２のキー情報を認証する第３の認証手段として機能するコンピュータを、前記サーバ装置とは別のサーバ装置に機能させることを特徴とする。

【００５０】

請求項２３に記載の発明によれば、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させるこ

とができる。

【００５１】

上記課題を解決するため、請求項２４に記載の発明は、請求項１９または２３に記載の通信機器認証用プログラムにおいて、前記別のサーバ装置は、前記第２のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定するように機能させることを特徴とする。

【００５２】

請求項２４に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【００５３】

請求項２５に記載の発明は、請求項１９乃至２４のいずれか一項に記載の通信機器認証用プログラムが記録されていることを特徴とする。

【００５４】

請求項１９に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成して通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【００５５】

請求項２０に記載の通信機器認証用プログラムが記録されている場合には、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳ

Ｌを使用しない認証の際、パスワードの代替とすることができる。

【００５６】

請求項２１に記載の通信機器認証用プログラムが記録されている場合には、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【００５７】

請求項２２に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【００５８】

請求項２３に記載の通信機器認証用プログラムが記録されている場合には、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【００５９】

請求項２４に記載の通信機器認証用プログラムが記録されている場合には、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【００６０】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

【００６１】

なお、以下に説明する実施形態は、パソコンなどの通信端末装置から通信手段としてのインターネットを介して入力されるユーザ特定情報に基づいて車両に搭載された通信端末装置である通信カーナビゲーション装置（以下、単に通信ナビと略称する。）を使用するユーザに対して認証を行い、その認証結果に基づいて

サーバ装置から通信ナビに地図データなどのデータを供給する通信機器認証システムに対して本発明を適用した場合の実施形態である。

【００６２】

図１は本発明に係る通信機器認証システムの第１実施形態の構成を示すブロック図、図２は図１のサーバ装置におけるデータベース部のデータ構造を示す説明図、図３は図２のデータ項目を示す説明図、図４は図１の通信端末装置であるパソコン、携帯電話機または通信カーナビゲーション装置の構成を示すブロック図、図５は図４のメモリ部に格納されるデータ構造を示す説明図である。

【００６３】

なお、図１ではパソコン、携帯電話機、通信カーナビゲーション装置がそれぞれ一台の例について説明するものの、実際にはパソコン、携帯電話機、通信ナビがそれぞれ複数台存在し、これらのパソコンまたは携帯電話機がサーバ装置と通信を行うことによりユーザ特定情報が認証され、その認証結果に基づいてサーバ装置から地図データなどのデータを通信ナビで受信するシステムである。また、以下の説明では、パソコン、携帯電話機、通信ナビをまとめて通信端末装置ともいう。

【００６４】

図１に示すように、本実施形態の通信機器認証システムは、通信サービス系サーバ装置（以下、単にサーバ装置と略称する。）１と通信端末装置２とが通信手段としてのインターネットＩＮを介して互いに送受信可能であり、通信端末装置２がパソコン３、携帯電話機４および通信ナビ５から構成されている。

【００６５】

通信端末装置２におけるパソコン３（または携帯電話機４）は、ポータルサイトからメールアドレスなどのユーザデータを入力してインターネットＩＮを介してサーバ装置１に送信する一方、このサーバ装置１から送信される申込み番号を受信するとともに、ポータルサイトからクレジット番号を入力してインターネットＩＮを介してサーバ装置１に送信する一方、このサーバ装置１から送信されるユーザＩＤ，パスワード，ライセンス番号などのユーザアカウント（ユーザ特定情報）を受信する。

【００６６】

他方、サーバ装置１は、パソコン３（または携帯電話機４）で受信したユーザアカウントが通信ナビ５からインターネットＩＮを介して送信された場合、このユーザアカウントを認証して通信ナビ５に対して第１のキー情報としてのアクセスキーを付与するとともに、このアクセスキーおよびユーザＩＤが通信ナビ５からインターネットＩＮを介して送信された場合、このアクセスキーを認証して通信ナビ５に対して第２のキー情報としてのセッションキーを付与し、このセッションキーが通信ナビ５からインターネットＩＮを介して送信された場合に通信ナビ５に対して必要な地図データなどを提供する。

【００６７】

次に、各構成部材の細部構成について説明する。

【００６８】

図１に示すように、サーバ装置１は、通信回線送受信部１１と、第１および第２の認証手段としての認証共通部１２と、セッションキーに基づくアクセスを所定時間内のみ許可するアクセス許可手段としての機能も有するシステム制御装置１３と、アプリケーション部１４と、ハードディスク装置などからなるデータベース部１５と、を備えて構成されている。

【００６９】

上記の構成において、サーバ装置１の通信回線送受信部１１は、インターネットＩＮから入力されるデータに対して予め設定されている処理を実行し、処理データとしてシステム制御装置１３に出力するとともに、このシステム制御装置１３から通信端末装置２に対して送信すべき処理データが送信されると、その処理データに対して予め設定されている処理を実行し、サーバ装置１のデータとしてインターネットＩＮを介して通信端末装置２へ送信する。

【００７０】

認証共通部１２は、上記アクセスキー、セッションキーなどを発行するとともに、これらの管理を実行する。

【００７１】

システム制御装置１３は、受信したデータまたはデータベース部１５に格納さ

れたデータに基づいて各部を制御するとともに、上記セッションキーに基づくアクセスを所定時間有効とする制御を実行する。

【００７２】

アプリケーション部１４は、ユーザの受信したデータを解析してデータベース部１５から必要なデータをシステム制御装置１３が取得するように指示する。

【００７３】

データベース部１５は、図２および図３に示すようにユーザの氏名，住所，電話番号，メールアドレス，申込み番号，クレジットカード番号，クレジットカード有効期限，ユーザＩＤ，パスワード，ライセンス番号，アクセスキー，メーカＩＤ，型番ＩＤ，ハードウェア番号，セッションキー，セッションキー有効時間の各データが記憶されるとともに、通信ナビ５の表示部に表示すべき地図データ、経路処理に用いられる種々のデータ、通信ナビ５の表示部に表示される地図上に示される地点の位置データおよびその地点の内容データなどを含み、ナビゲーション処理の実行に必要な地点データ、各通信ナビ５を使用しているユーザについてのデータであるユーザデータなど、ナビゲーションシステムとして実行されるナビゲーション処理に必要な全てのデータを記憶しており、これらのデータを必要に応じてシステム制御装置１３に出力する。

【００７４】

次に、通信端末装置２は、図４に示すように通信回線送受信部１６と、システム制御部１７と、データ入力部である操作部１８と、表示部１９と、メモリ部２０と、を備えて構成されている。

【００７５】

上記の構成において、通信回線送受信部１６は、インターネットＩＮから入力する端末データに対して予め設定されている入力処理を実行し、処理端末データとしてシステム制御部１７に出力するとともに、このシステム制御部１７からサーバ装置１に対して送信すべき処理端末データが送信されると、その処理端末データに対して予め設定されている出力処理を実行し、端末データとしてインターネットＩＮを介してサーバ装置１へ出力する。

【００７６】

システム制御部１７は、受信したデータまたはメモリ部２０に格納されたデータに基づいて各部を制御する。

【００７７】

操作部１８は、表示部１９に表示する地図の指定または目的地の設定などのナビゲーション処理について指定すると、その指定に対応する入力データを生成してシステム制御部１７に出力する。

【００７８】

表示部１９は、地図、地図上に示される地点の位置および経路などを表示する。

【００７９】

メモリ部２０は、図５に示すようにサーバ装置１から送信されてきたユーザＩＤ，パスワード，ライセンス番号などのユーザアカウント（ユーザ特定情報）や、アクセスキー、セッションキーが記憶される他、地図データなど、一時的に記憶しておくべきデータについてシステム制御部１７から出力されて一時的に記憶され、必要に応じて読み出されて表示などの処理に供される。

【００８０】

次に、上述した第１実施形態の通信機器認証システムにおいて実行される通信ナビ接続までの処理の概要を図６に基づいて説明する。

【００８１】

図６において、通信ナビ接続までの処理は、まずユーザによりパソコン３のポータルサイトからメールアドレスなどを入力してＳＳＬを用いてサーバ装置１に申込み手続を実行すると、サーバ装置１は申込み番号を発行し、この申込み番号を電子メールによりパソコン３に送信する（ステップＳ１）。

【００８２】

次いで、パソコン３のポータルサイトからクレジット番号などを入力してＳＳＬを用いてサーバ装置１にユーザ登録手続を実行すると、サーバ装置１ではユーザアカウント（ユーザＩＤ、パスワード、ライセンス番号）を発行し、これらのユーザアカウントはＳＳＬを用いてパソコン３に送信する（ステップＳ２）。

【００８３】

なお、ステップＳ１，Ｓ２においては、パソコン３以外に携帯電話機４を使用してもよく、これらを持たないユーザは書面の郵送または電話による通知にてサーバ装置１側から上記ユーザアカウントを受信する。

【００８４】

さらに、ユーザは受信したユーザアカウント（ユーザＩＤ、パスワード、ライセンス番号）を通信ナビ５に入力してインターネットＩＮを介してサーバ装置１に簡易サインアップ用データとして送信すると、サーバ装置１ではユーザアカウントを認証してアクセスキーを生成し、このアクセスキーを通信ナビ５に送信する（ステップＳ３）。

【００８５】

そして、ユーザは受信したアクセスキーおよびユーザＩＤを通信ナビ５に入力してインターネットＩＮを介してサーバ装置１に送信すると、サーバ装置１ではアクセスキーおよびユーザＩＤを認証してセッションキーを生成し、このセッションキーを通信ナビ５に送信する（ステップＳ４）。

【００８６】

次いで、ユーザは受信したセッションキーおよびユーザＩＤを通信ナビ５に入力してインターネットＩＮを介してサーバ装置１に送信すると、サーバ装置１では通信ナビ５に対して必要な地図データなどを提供するサービスを開始する（ステップＳ５）。

【００８７】

そして、サーバ装置１は、セッションキーの有効時間（例えば５分に設定）切れになるまで通信ナビ５に対して必要な地図データなどを提供し（ステップＳ５；ＮＯ）、セッションキーの有効時間に達する（ステップＳ５；ＹＥＳ）と、ステップＳ４に戻り、ユーザは再度セッションキーを取得する。

【００８８】

次に、上述した図６の各ステップにおいて実行される処理の詳細を図７～図１１に基づいて説明する。

【００８９】

図７は図６のステップＳ１の詳細を示し、ユーザ登録（申込み番号付与）処理を実行するためのフローチャートである。

【００９０】

図７に示すように、ユーザ登録（申込み番号付与）処理は、まずユーザによりパソコン３のポータルサイトをサーバ装置１側に接続すると、サーバ装置１側はこれを受信して接続し、ユーザはパソコン３の表示部１９において「初めて登録する」を選択する（ステップＳ１１～Ｓ１４）。

【００９１】

そして、ユーザはパソコン３からメールアドレスや氏名などのユーザ情報を入力し、このユーザ情報をサーバ装置１側にＳＳＬを用いて送信する（ステップＳ１５，Ｓ１６）。すると、サーバ装置１は図２および図３に示すようなユーザ情報を受信して登録するとともに、申込み番号を発行し、この申込み番号および決済画面ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を電子メールにてユーザのパソコン３に送信し、このパソコン３が申込み番号および決済画面ＵＲＬを受信する（ステップＳ１７～Ｓ２０）。

【００９２】

図８は図６のステップＳ２の詳細を示し、ユーザ登録（ユーザアカウント付与）処理を実行するためのフローチャートである。

【００９３】

図８に示すように、ユーザ登録（ユーザアカウント付与）処理は、まずユーザによりパソコン３の決済画面ＵＲＬをサーバ装置１側に接続すると、サーバ装置１側はこれを受信して接続し、パソコン３に申込み番号入力画面を表示する（ステップＳ２１～Ｓ２４）。

【００９４】

そして、ユーザはパソコン３から申込み番号を入力し、この申込み番号情報をサーバ装置１側にＳＳＬを用いて送信する（ステップＳ２５，Ｓ２６）。すると、サーバ装置１は申込み番号情報を受信し、この申込み番号情報を認証した後、決済画面情報をユーザのパソコン３にＳＳＬを用いて送信し、このパソコン３に

決済画面を表示させる（ステップＳ２７～Ｓ２９）。

【００９５】

次いで、ユーザはパソコン３に表示された決済画面にクレジットカード番号やカード有効期限などの必要項目を入力し、これらの情報をサーバ装置１側にＳＳＬを用いて送信する（ステップＳ３０，Ｓ３１）。サーバ装置１では、ステップＳ３２，Ｓ３３で必要項目の情報を受信した後にユーザ側に与信し、その与信が成功した場合（ステップＳ３４；ＹＥＳ）には、クレジット番号およびカード有効期限を登録した後、ユーザアカウント（ユーザＩＤ、パスワード、ライセンス番号を発行する（ステップＳ３５，Ｓ３６）。一方、与信が不成功の場合（ステップＳ３４；ＮＯ）には、ステップＳ３７でユーザ側に再入力を要求してステップＳ３０に戻る。

【００９６】

また、サーバ装置１は、発行されたユーザＩＤ、パスワード、ライセンス番号をユーザのパソコン３にＳＳＬを用いて送信するとともに、電子メールでも同時に通達した後、データベース部１５に上記ユーザアカウントを保存する（ステップＳ３８，Ｓ３９）。

【００９７】

さらに、ユーザのパソコン３は、サーバ装置１から送信されてきたユーザＩＤ、パスワード、ライセンス番号を受信して表示部１９に表示する（ステップＳ４０，Ｓ４１）。

【００９８】

図９は図６のステップＳ３の詳細を示し、簡易サインアップ処理を実行するためのフローチャートである。なお、上記簡易サインアップ処理は、ユーザが用いる通信ナビ５のハードウェア番号を取得することができない場合であって、ユーザ登録（クレジットカード番号入力）済みであることが条件である。

【００９９】

図９に示すように、簡易サインアップ処理は、まず通信ナビ５の表示部１９に初期登録画面を表示してユーザアカウント（ユーザＩＤ、パスワード、ライセンス番号）を入力する（ステップＳ５１，Ｓ５２）。次いで、これらユーザＩＤ、

パスワード、ライセンス番号を簡易サインアップ用データとして通信ナビ５に付与されているメーカＩＤ、型番ＩＤとともに、インターネットＩＮを介してサーバ装置１に送信する（ステップＳ５３）。

【０１００】

このステップＳ５３において、ＳＳＬを使用せずにパスワードを通信回線に重畳させるのは、簡易サインアップ用データ送信時の１回のみである。この簡易サインアップ用データ送信時にパスワードを通信回線に重畳させない方法を採用する場合には、通信ナビ５およびサーバ装置１の双方で同一の暗号化の関数（ハッシュ関数）を備え、通信ナビ５で暗号化したパスワードをサーバ装置１へ送信し、サーバ装置１側で予め登録しておいたパスワードを暗号化したものと一致するか否かを判定するような方法が挙げられる。

【０１０１】

サーバ装置１は、上記簡易サインアップ用データを受信した後、サーバ装置１にユーザＩＤは登録されているか、ユーザＩＤおよびパスワードは有効か、アクセスキーは未発行かを認証する（ステップＳ５４，Ｓ５５）。認証結果がＯＫの場合には、ステップＳ５６でアクセスキーを生成した後、ステップＳ５７に進む。

【０１０２】

一方、認証結果がＮＧの場合には、ステップＳ５８でエラーコードを生成した後、ステップＳ５７に進む。なお、上記アクセスキーは生成する度に変わり、既に登録済みのユーザＩＤに対してアクセスキーを生成する場合（端末譲渡時など）も、異なるアクセスキーを生成する。これにより、同一ユーザアカウントを複数の通信ナビ５で使用するのを防止することができる。

【０１０３】

次に、ステップＳ５７では、サーバ装置１から通信ナビ５にアクセスキーまたはエラーコードを送信する。通信ナビ５では、アクセスキーを受信したか否かを判断（ステップＳ５９）し、アクセスキーを受信した場合（ステップＳ５９；ＹＥＳ）には、登録確認用データとしてユーザＩＤおよびアクセスキーをサーバ装置１に送信する（ステップＳ６０）。一方、アクセスキーを受信しない場合（ス

テップＳ５９；ＮＯ）には、処理を終了する。

【０１０４】

ところで、サーバ装置１において発行したアクセスキーが何等かの障害（通信不能、圏外など）によって最悪の場合、通信ナビ５側に送信されない可能性もある。したがって、アクセスキーが通信ナビ５側に送信されなかった場合、そのユーザはサーバ接続時に簡易サインアップをやり直す必要がある。しかも、サーバ装置１側ではアクセスキー既存エラーを返信するため、エラー処理に手間を要することになる。そこで、ステップＳ６０において、通信ナビ５のアプリケーションが受信したアクセスキーをユーザＩＤとともにサーバ装置１へ送信する。これにより、アクセスキーの受け渡しの確認が可能となる。

【０１０５】

サーバ装置１は、ステップＳ６１でアクセスキーおよびユーザＩＤを受信し、アクセスキーおよびユーザＩＤの有効性を照会（ステップＳ６２）し、照会結果がＯＫの場合には、ステップＳ６３でメーカＩＤ、型番ＩＤおよびアクセスキーを新規に登録した後、ステップＳ６４に進む。なお、サーバ装置１側では、ユーザＩＤ、パスードおよびライセンス番号は、既に登録済みである。一方、照会結果がＮＧの場合には、ステップＳ６５でエラーコードを生成した後、ステップＳ６４に進む。

【０１０６】

次に、ステップＳ６４では、サーバ装置１から通信ナビ５に登録終了通知またはエラーコードを送信する一方、通信ナビ５では、これら登録終了通知またはエラーコードを受信してこれらを認証する（ステップＳ６６）。そして、エラーコードを受信した場合（ステップＳ６７；ＹＥＳ）には、処理を終了する一方、エラーコードを受信しない場合（ステップＳ６７；ＮＯ）には、通信ナビ５のメモリ部２０にユーザＩＤ、アクセスキーおよびライセンス番号を格納して処理を終了する（ステップＳ６８）。ここで、アクセスキーはユーザに対して目視不可能な形態でメモリ部２０に格納し、パスワードはメモリ部２０に保存しないこととする。

【０１０７】

図１０は図６のステップＳ４の詳細を示し、セッションキー取得処理を実行するためのフローチャートである。

【０１０８】

図１０に示すように、セッションキー取得処理は、まず通信ナビ５からセッションキー取得用データとしてユーザＩＤおよびアクセスキーをサーバ装置１へ送信する（ステップＳ７１）。このサーバ装置１は、ユーザＩＤおよびアクセスキーを受信（ステップＳ７２）し、その受信したユーザＩＤが登録済みか、ユーザＩＤとアクセスキーとが対応するかをそれぞれ認証（ステップＳ７３）し、ユーザＩＤが登録済みであって、ユーザＩＤとアクセスキーとが対応する場合（ステップＳ７３；ＯＫ）には、ステップＳ７４で有効時間（例えば５分）が予め設定されたセッションキーを生成した後、セッションキーおよびその有効時間を登録する（ステップＳ７５）。

【０１０９】

一方、ユーザＩＤが未登録であって、ユーザＩＤとアクセスキーとが対応しない場合（ステップＳ７３；ＮＧ）には、ステップＳ７６でエラーコードを生成した後、ステップＳ７７に進む。

【０１１０】

次に、ステップＳ７７では、サーバ装置１から通信ナビ５にセッションキー、その有効時間およびエラーコードを送信する。通信ナビ５では、ステップＳ７８でこれらの情報を受信した後、セッションキーを受信したか否かを判断（ステップＳ７９）し、セッションキーを受信した場合（ステップＳ７９；ＹＥＳ）には、通信ナビ５のメモリ部２０にユーザＩＤ、アクセスキーおよびライセンス番号とともに、セッションキー、その有効時間を格納（ステップＳ８０）して処理を終了する。また、セッションキーを受信しない場合（ステップＳ７９；ＮＯ）には、処理を終了する。

【０１１１】

なお、これら一連の処理において、セッションキー取得時は、ユーザが通常アクセスを開始した場合、通信ナビ５のメモリ部２０にセッションキーを格納していない場合、セッションキーエラー時、またはセッションキー有効時間超過エラ

一時のそれぞれに該当する場合には、セッションキー取得開始処理を実行する。

【０１１２】

図１１は図６のステップＳ５，Ｓ６の詳細を示し、通常アクセス認証処理を実行するためのフローチャートである。

【０１１３】

図１１に示すように、通常アクセス認証処理は、まず通信ナビ５からユーザＩＤおよびセッションキーをサーバ装置１に送信して通常アクセスを開始する（ステップＳ８１）。サーバ装置１では、これらの情報を受信してユーザＩＤは登録されているか、ユーザＩＤおよびセッションキーは有効かを判断するとともに、セッションキー有効時間の確認、サービス契約の確認などの認証処理を実行する（ステップＳ８２，Ｓ８３）。この認証結果がＯＫの場合には、ステップＳ８４で地図データなどのサービス開始許可コードを生成する一方、認証結果がＮＧの場合には、ステップＳ８５でエラーコードを生成した後、ステップＳ８６に進む。

【０１１４】

ステップＳ８６では、サーバ装置１から通信ナビ５にサービス開始許可コードまたはエラーコードのいずれかのコードを送信する。通信ナビ５では、ステップＳ８７でこれらサービス開始許可コードまたはエラーコードのいずれかを受信した後、エラーコードを受信したか否かを判断（ステップＳ８８）し、エラーコードを受信しない場合（ステップＳ８８；ＮＯ）には、サービス開始許可コードを受信したことになるので、サーバ装置１に対してサービス開始の旨の情報を送信する一方、サーバ装置１から地図データなどの各種コンテンツが送信される（ステップＳ８９，Ｓ９０）。

【０１１５】

また、エラーコードを受信した場合（ステップＳ８８；ＹＥＳ）には、ステップＳ９１でセッションキーがエラーか否かを判断し、セッションキーがエラーの場合（ステップＳ９１；ＹＥＳ）には、上述した図１０に示すセッションキー取得処理に戻る。セッションキーがエラーでない場合（ステップＳ９１；ＮＯ）には、ステップＳ９２でエラーに対処して処理を終了する。

【０１１６】

一方、サーバ装置１では、ダウンロードが完了したか否かを判断する（ステップＳ９３）。すなわち、通信ナビ５に送信すべきコンテンツの送信が完了したか否かを判断し、完了しない場合（ステップＳ９３；ＮＯ）には、ステップＳ９４でセッションキーの有効時間（例えば５分に設定）を確認した後、上述したステップＳ８３の照会処理に戻る。また、ダウンロードが完了した場合（ステップＳ９３；ＹＥＳ）には、サーバ装置１の処理を終了する。

【０１１７】

ここで、セッションキーの有効時間は、例えば５分に設定に設定したが、これに限らず通信ナビ５に送信するデータのサイズや内容に基づいて変化させたり、延長処理したりしてもよい。

【０１１８】

また、通信ナビ５では、サーバ装置１からの地図データなどの各種コンテンツのダウンロードが完了したか否かを判断する（ステップＳ９５）。すなわち、サーバ装置１から受信すべきコンテンツの受信が全て完了したか否かを判断し、完了しない場合（ステップＳ９５；ＮＯ）には、上述したステップＳ８７の受信処理に戻る。また、コンテンツの受信が完了した場合（ステップＳ９５；ＹＥＳ）には、通信ナビ５の処理を終了する。

【０１１９】

以上説明したように、本実施形態の通信機器認証システムによれば、パソコン３から送信されるユーザアカウントを認証し、当該ユーザアカウントに基づいてアクセスキーを生成してサーバ装置１から通信ナビ５に送信する認証共通部１２と、通信ナビ５から送信されるアクセスキーを認証し、当該アクセスキーに基づいて地図データなどに対してアクセスするセッションキーを生成してサーバ装置１から通信ナビ５に送信する認証共通部１２と、通信ナビ５からサーバ装置１へのセッションキーに基づくアクセスを所定時間内のみ許可するシステム制御装置１３とを備えたことにより、地図データなどにアクセスするためのセッションキーに有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置２であってもデー

タ転送速度を低下させることなく、サーバ装置１への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１２０】

また、本実施形態によれば、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０１２１】

さらに、本実施形態によれば、通信端末装置５は、通信ナビ５、パソコン３、携帯電話機４、携帯情報端末のうち、選択された一種であることから、汎用性を高めることができる。

【０１２２】

図１２および図１３は本発明に係る通信機器認証システムの第２実施形態における通信端末追加処理を示すフローチャート、図１４（Ａ）は第２実施形態において単一アクセスキー使用時のデータ構造を示す説明図，図１４（Ｂ）は第２実施形態において１アクセスキーを複数の通信端末装置で使用する場合のデータ構造を示す説明図である。

【０１２３】

本実施形態は、１つのアクセスキーに対して複数台の通信端末装置を登録する場合の例を示している。具体的には、例えば一人が複数台の車両を保有し、各車両にそれぞれ通信ナビを搭載したとき、各通信ナビのアクセスキーを共通にする場合である。

【０１２４】

また、本実施形態の説明では、第１の車両が第１の通信ナビを搭載し、第２の車両が第２の通信ナビを搭載しており、第１の通信ナビに対してユーザＩＤ、パスワード、ライセンス番号およびアクセスキーが既に付与され、このアクセスキーを第２の通信ナビに対しても登録する例について説明する。

【０１２５】

図１２に示すように、通信端末追加処理は、まず第２の通信ナビ５の表示部１

９に初期登録画面を表示して第１の通信ナビ５に予め付与されているユーザアカウント（ユーザＩＤ、パスワード、ライセンス番号）を入力する（ステップＳ１０１，Ｓ１０２）。次いで、これらユーザＩＤ、パスワード、ライセンス番号を簡易サインアップ用データとして第２の通信ナビ５に付与されているメーカＩＤ、型番ＩＤとともにインターネットＩＮを介してサーバ装置１に送信する（ステップＳ１０３）。

【０１２６】

サーバ装置１は、上記簡易サインアップ用データを受信した後、サーバ装置１にユーザＩＤは登録されているか、ユーザＩＤおよびパスワードは有効か、アクセスキーは未発行かをそれぞれ認証する（ステップＳ１０４，Ｓ１０５）。認証結果がＮＧの場合には、ステップＳ１０６で追加登録可能か否かを判断し、追加登録不可の場合（ステップＳ１０６；ＮＯ）には、ステップＳ１０７でエラーコードを生成した後、ステップＳ１０８に進む。

【０１２７】

ここで、ステップＳ１０６の追加登録可能か否かの判断処理は、追加登録可能な車両の台数の制限や、サービス提供者の設定によって追加登録ができない場合を考慮して設けたのであり、例えばサービス提供者の設定によって追加登録可能台数が２台まで無料で、３台目を追加しようとした場合は、ステップＳ１０６でＮＯとなり、既に登録済みの通信ナビ５を消去（上書き）するか、登録を断念する。なお、この場合、サービス提供者の仕様によっては、追加料金を支払うことで追加登録が可能となるようにしてもよい。

【０１２８】

ステップＳ１０８では、サーバ装置１から第２の通信ナビ５に追加登録不可であって、上書き（車両の乗換え）または追加登録する情報を送信する。ここで、１アクセスキーに対して１通信ナビしか登録することができない場合や、１アクセスキーに対して登録することのできる通信ナビ数が既に限度に達している場合には、一旦追加登録不可の案内をユーザに送信する。また、既に登録済みの通信ナビ５を消去し、新たに追加登録するか、または追加料金を支払うことにより、追加登録を可能にしてもよい。

【０１２９】

一方、通信ナビ５は、上書きまたは追加登録する情報を受信して上書きか否かを判断する（ステップＳ１０９，Ｓ１１０）。上書きの場合には、サーバ装置１に対して登録済み端末（通信ナビ）を問い合わせする（ステップＳ１１１）。また、ステップＳ１１０で上書きでない場合には、ステップＳ１１２で追加登録するか否かを判断し、追加登録する場合（ステップＳ１１２；ＹＥＳ）には、ステップＳ１１３でサーバ装置１に対して追加条件を問い合わせする一方、追加登録しない場合（ステップＳ１１２；ＮＯ）には、ステップＳ１１４でキャンセルコードを生成する。そして、通信ナビ５は、これら登録済み端末（通信ナビ）問合せ情報、追加条件問合せ情報またはキャンセルコードをサーバ装置１に送信する（ステップＳ１１５）。

【０１３０】

サーバ装置１では、それらの問い合わせ情報またはキャンセルコードを受信する（ステップＳ１１６）。次いで、ステップＳ１１７で問合せ情報が上書きか否かを判断し、上書きの場合（ステップＳ１１７；ＹＥＳ）には、ステップＳ１１８で登録済み端末（通信ナビ）を検索し、上書きでない場合（ステップＳ１１７；ＮＯ）には、ステップＳ１１９で追加登録するか否かを判断し、追加登録する場合（ステップＳ１１９；ＹＥＳ）には、ステップＳ１２０で追加条件を検索（参照）する。すなわち、ステップＳ１２０では、端末（通信ナビ）を追加登録場合の条件（追加料金や契約内容など）を検索し、その検索結果を通信ナビ５側に送信する（ステップＳ１２１）。

【０１３１】

通信ナビ５は、登録済み端末（通信ナビ）の検索結果および追加条件の検索結果を受信する（ステップＳ１２２）。そして、図１３に示すように、通信ナビ５は、上書き処理の場合（ステップＳ１２３；ＹＥＳ）には、ステップＳ１２４で上書き（消去）する端末（通信ナビ）を指定する一方、上書き処理でない場合（ステップＳ１２３；ＮＯ）には、ステップＳ１２５で追加処理か否かを判断し、追加処理の場合（ステップＳ１２５；ＹＥＳ）で、追加条件がＯＫの場合（ステップＳ１２６；ＹＥＳ）には、追加処理コードを生成する（ステップＳ１２７）

。また、ステップＳ１２５で追加処理ではない場合（ステップＳ１２５；ＮＯ）や、追加条件がＯＫでない場合（ステップＳ１２６；ＮＯ）には、キャンセル処理を実行する（ステップＳ１２８）。

【０１３２】

さらに、通信ナビ５は、ステップＳ１２４で指定された上書き（消去）する端末（通信ナビ）、ステップＳ１２７で生成された追加処理コードをサーバ装置１に送信する（ステップＳ１２９）。

【０１３３】

サーバ装置１は、ステップＳ１３０で上書き（消去）する端末（通信ナビ）の情報および追加処理コードを受信し、上書き処理の場合（ステップＳ１３１；ＹＥＳ）には、ステップＳ１３２で指定端末（通信ナビ）無効処理を実行する一方、上書き処理でない場合（ステップＳ１３１；ＮＯ）には、ステップＳ１３３で追加処理かを判断し、追加処理の場合（ステップＳ１３３；ＹＥＳ）には、追加手続および処理を実行する（ステップＳ１３４）。そして、追加処理でない場合（ステップＳ１３３；ＮＯ）には、キャンセル処理を実行する（ステップＳ１３５）。

【０１３４】

ここで、端末（通信ナビ）の追加処理登録を実行し、１ユーザＩＤに対して複数アクセスキーを発行する場合は、図１４（Ａ）に示すようなデータ構造となり、１アクセスキーを複数の通信ナビを所有する場合は、図１４（Ｂ）に示すデータ構造となる。そして、通信ナビを追加登録した後、ユーザの通信系サービスに対する契約内容についても更新を行う。

【０１３５】

また、サーバ装置１は、ステップＳ１３２で指定端末（通信ナビ）無効処理を実行した後、およびステップＳ１３４で追加手続および処理を実行した後は、アクセスキーを生成し、このアクセスキーまたはキャンセル処理情報を通信ナビ５に送信する（ステップＳ１３６，Ｓ１３７）。なお、図１２に示すステップＳ１０５で認証結果がＯＫの場合、およびステップＳ１０６で追加登録可能な場合には、ステップＳ１３６で直接アクセスキーを生成する。

【０１３６】

一方、通信ナビ５は、ステップＳ１３８でアクセスキーまたはキャンセル処理情報を受信し、アクセスキーか否かを判断し、アクセスキーの場合（ステップＳ１３９；ＹＥＳ）には、登録確認用データをサーバ装置１に送信する（ステップＳ１４０）。また、アクセスキーでない場合（ステップＳ１３９；ＮＯ）には、通信ナビ５の全体の処理を終了する。

【０１３７】

サーバ装置１は、ステップＳ１４１で登録確認用データを受信し、この登録確認用データを照会し、ＯＫの場合には該当するアクセスキーを登録する（ステップＳ１４２，Ｓ１４３）。また、照会結果がＮＧの場合にはエラーコードを生成する（ステップＳ１４４）。そして、サーバ装置１は、アクセスキーまたはエラーコードを通信ナビ５に送信する（ステップＳ１４５）。

【０１３８】

通信ナビ５は、ステップＳ１４６でアクセスキーまたはエラーコードを受信し、エラーコードの場合（ステップＳ１４７；ＹＥＳ）には、通信ナビ５の全体の処理を終了する。また、エラーコードでない場合（ステップＳ１４７；ＮＯ）には、アクセスキーをメモリ部２０にデータとして保存する（ステップＳ１４９）。

【０１３９】

このように本実施形態によれば、同一ユーザから別の通信ナビ５を用いてユーザアカウントが送信された場合、そのユーザアカウントに基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信ナビ５を用いることができる。

【０１４０】

図１５は本発明に係る通信機器認証システムの第３実施形態における簡易サインアップ処理を示すフローチャートである。なお、本実施形態の簡易サインアップ処理は、ユーザが用いる通信ナビ５の装置識別情報としてのハードウェア番号を取得することができる場合であって、ユーザ登録（クレジットカード番号入力

）済みであることが条件である。

【０１４１】

図１５に示すように、簡易サインアップ処理は、まず通信ナビ５の表示部１９に初期登録画面を表示してユーザアカウント（ユーザＩＤ、パスワード）を入力する（ステップＳ１５１，Ｓ１５２）。なお、本実施形態のようにハードウェア番号を取得することができる場合には、ユーザアカウント入力時にライセンス番号が不要になる。但し、ハードウェア番号は重複しないことが前提条件である。

【０１４２】

次いで、これらユーザＩＤ、パスワード、ハードウェア番号を簡易サインアップ用データとして通信ナビ５に付与されているメーカＩＤ、型番ＩＤとともにインターネットＩＮを介してサーバ装置１に送信する（ステップＳ１５３）。

【０１４３】

サーバ装置１は、上記簡易サインアップ用データを受信した後、サーバ装置１にユーザＩＤは登録されているか、ユーザＩＤおよびパスワードは有効か、アクセスキーは未発行かをそれぞれ認証する（ステップＳ１５４，Ｓ１５５）。認証結果がＯＫの場合には、ステップＳ１５６でアクセスキーを生成した後、ステップＳ１５７に進む。一方、認証結果がＮＧの場合には、ステップＳ１５８でエラーコードを生成した後、ステップＳ１５７に進む。

【０１４４】

次に、ステップＳ１５７では、サーバ装置１から通信ナビ５にアクセスキーまたはエラーコードを送信する。通信ナビ５では、アクセスキーを受信したか否かを判断（ステップＳ１５９）し、アクセスキーを受信した場合（ステップＳ１５９；ＹＥＳ）には、登録確認用データとしてユーザＩＤおよびアクセスキーをサーバ装置１に送信する（ステップＳ１６０）。一方、アクセスキーを受信しない場合（ステップＳ１５９；ＮＯ）には、処理を終了する。

【０１４５】

サーバ装置１は、ステップＳ１６１でアクセスキーおよびユーザＩＤを受信し、アクセスキーおよびユーザＩＤの有効性を照会（ステップＳ１６２）し、照会結果がＯＫの場合には、ステップＳ１６３でハードウェア番号、メーカＩＤ、型

番ＩＤおよびアクセスキーを新規に登録した後、ステップＳ１６４に進む。なお、サーバ装置１側では、ユーザＩＤおよびライセンス番号などのユーザアカウントは、既に登録済みであり、ステップＳ１６３でハードウェア番号（機器番号）を登録することで、通信ナビ５の譲渡時などに通信ナビ５の特定が可能となる。一方、照会結果がＮＧの場合には、ステップＳ１６５でエラーコードを生成した後、ステップＳ１６４に進む。

【０１４６】

次に、ステップＳ１６４では、サーバ装置１から通信ナビ５に登録終了通知またはエラーコードを送信する一方、通信ナビ５では、これらの登録終了通知またはエラーコードを受信してこれらを認証する（ステップＳ１６６）。そして、エラーコードを受信した場合（ステップＳ１６７；ＹＥＳ）には、処理を終了する一方、エラーコードを受信しない場合（ステップＳ１６７；ＮＯ）には、通信ナビ５のメモリ部２０にユーザＩＤおよびアクセスキーを格納して処理を終了する（ステップＳ１６８）。ここで、アクセスキーはユーザに対して目視不可能な形態でメモリ部２０に格納し、パスワードはメモリ部２０に保存しないこととする。

【０１４７】

このように本実施形態によれば、通信ナビ５に予め設定された装置識別情報としてのハードウェア番号を入力しておき、このハードウェア番号をメーカＩＤ、型番ＩＤ、アクセスキーおよびユーザアカウントとともにサーバ装置１で受信可能としたことにより、サーバ装置１がハードウェア番号も受信することで、セキュリティを一段と高めることができる。

【０１４８】

図１６は本発明に係る通信機器認証システムの第４実施形態の構成を示すブロック図、図１７は第４実施形態の処理を示すフローチャートである。なお、図１６において図１と同一の構成部材には、同一の符号を付して説明する。

【０１４９】

本実施形態は、サーバ装置１により生成された第２のキー情報としてのセッションキーを認証する第３の認証手段としての認証共通部を、サーバ装置１とは別

のサーバ装置としての外部ＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）１ａに設けた例である。

【０１５０】

外部ＡＳＰ１ａは、図１６に示すようにサーバ装置１と同様に通信回線送受信部１１ａと、サーバ装置１により生成されたセッションキーを認証する第３の認証手段としての認証共通部１２ａと、システム制御装置１３ａと、アプリケーション部１４ａと、ハードディスク装置などからなるデータベース部１５ａとを備え、インターネットＩＮを介してサーバ装置１および通信端末装置２と送受信可能に構成されている。

【０１５１】

外部ＡＳＰ１ａの通信回線送受信部１１ａは、インターネットＩＮから入力されるプロバイダ信号に対して予め設定されている処理を実行し、処理信号としてシステム制御装置１３ａに出力するとともに、このシステム制御装置１３ａからサーバ装置１または通信端末装置２に対して送信すべき処理プロバイダ信号が出力されると、その処理プロバイダ信号に対して予め設定されている処理を実行し、プロバイダ信号としてインターネットＩＮを介してサーバ装置１または通信端末装置２へ出力する。

【０１５２】

認証共通部１２ａは、認証キャッシュを参照することで、ユーザＩＤおよびセッションキーの有効を判断し、サーバ装置１により生成されたセッションキーを認証するとともに、これらの管理を実行する。

【０１５３】

システム制御装置１３ａは、受信したデータまたはデータベース部１５に格納されたデータに基づいて各部を制御するとともに、上記セッションキーに基づくアクセスを所定時間有効とする制御を実行する。

【０１５４】

アプリケーション部１４ａは、受信したデータを解析してデータベース部１５ａから必要なデータをシステム制御装置１３ａが取得するように指示する。

【０１５５】

データベース部１５ａは、ユーザＩＤ、セッションキーおよびセッションキーの有効時間のデータ、通信ナビ５の表示部に表示すべき地図データ、経路処理に用いられる種々のデータ、通信ナビ５の表示部に表示される地図上に示される地点の位置データおよびその地点の内容データなどを含み、ナビゲーション処理の実行に必要な地点データ、各通信ナビ５を使用しているユーザについてのデータであるユーザデータなど、ナビゲーションシステムとして実行されるナビゲーション処理に必要な全てのデータを記憶しており、これらのデータを必要に応じてシステム制御装置１３ａに出力する。

【０１５６】

なお、サーバ装置１および通信端末装置２の構成および機能は、前記第１実施形態と同様であるので、その説明を省略する。

【０１５７】

次に、上述した本実施形態の通信機器認証システムにおいて実行される処理の概要を図１７に基づいて説明する。なお、セッションキー取得時の処理および通常アクセス時の処理は、それぞれ図１０および図１１と同様である。

【０１５８】

図１７に示すように、本実施形態の処理は、まず通信ナビ５からインターネットＩＮを介してサーバ装置１にセッションキーの取得を要求する（ステップＳ１７１）。このサーバ装置１は、セッションキー取得要求の情報を受信し、有効時間（例えば５分）が予め設定されたセッションキーを生成する（ステップＳ１７２，Ｓ１７３）。そして、通信ナビ５は、ステップＳ１７４でサーバ装置１からセッションキー、その有効時間の情報を受信する。なお、ステップＳ１７３，Ｓ１７４において、セッションキーの取得を要求してきた通信ナビ５が依然として有効時間内のセッションキーを有している場合は、改めてセッションキーを生成しない。この場合には、通信ナビ５が格納しているセッションキーを継続して使用する指示の情報を送信する。

【０１５９】

通信ナビ５は、セッションキー、その有効時間などの情報を受信した後、外部ＡＳＰ１ａにユーザＩＤおよびセッションキーなどの情報を送信してサービスを

要求する（ステップＳ１７４，Ｓ１７５）。

【０１６０】

外部ＡＳＰ１ａは、ステップＳ１７６でユーザＩＤおよびセッションキーなどの情報を受信した後、ステップＳ１７７に移行して認証キャッシュを参照することで、ユーザＩＤおよびセッションキーの有効を判断する。つまり、初めてアクセスした場合は、このステップＳ１７７においてＮＧという判断になる。そして、セッションキーが有効時間内で２回目以降のアクセスであれば、ＯＫという判断になる。

【０１６１】

ステップＳ１７７においてＮＧの場合には、ステップＳ１７８でユーザＩＤ、セッションキー、サービスＩＤおよび外部ＡＳＰ１ａのＩＤの各情報を外部認証用データとしてサーバ装置１に送信する。

【０１６２】

サーバ装置１は、外部認証用データを受信した後、ユーザＩＤ、セッションキー、サービスＩＤおよび外部ＡＳＰ１ａのＩＤの各情報を認証する（ステップＳ１７９，Ｓ１８０）。この認証判断結果がＮＧの場合には、ステップＳ１８１でエラーコードを生成した後、ステップＳ１８２に進む。認証判断結果がＯＫの場合には、直接ステップＳ１８２に進む。このステップＳ１８２では、サーバ装置１から外部ＡＳＰ１ａに外部認証用データまたはエラーコードに送信する。

【０１６３】

外部ＡＳＰ１ａは、外部認証用データまたはエラーコードを受信した後、エラーコードか否かを判断する（ステップＳ１８３，Ｓ１８４）。エラーコードの場合（ステップＳ１８４；ＹＥＳ）には、外部ＡＳＰ１ａから通信ナビ５にエラーコードを送信する。この通信ナビ５はエラーコードを受信し、そのエラーコードがセッションキーエラーか否かを判断する（ステップＳ１８５，Ｓ１８６）。セッションキーエラーの場合（ステップＳ１８６；ＹＥＳ）には、ステップＳ１７１に戻り、通信ナビ５からサーバ装置１に再度セッションキー取得要求を実行する。また、セッションキーエラーでない場合（ステップＳ１８６；ＮＯ）には、ステップＳ１８７でエラーに対処した後、後述するＤＬＬ（Ｄｙｎａｍｉｃ　Ｌ

ｉｎｋ　Ｌｉｂｒａｒｙ）完了の判断処理（ステップＳ１８２）に移行する。

【０１６４】

一方、ステップＳ１８４でエラーコードでない場合（ステップＳ１８４；ＮＯ）には、ステップＳ１８８でユーザＩＤ、セッションキー、その有効時間を外部ＡＳＰ１ａに登録する。この有効時間は、セッションキー取得時刻にセッションキー許可残り時間を加えた時間となる。このように外部ＡＳＰ１ａでのセッションキー有効時間は、残り時間を採用することにより、サーバ装置１と外部ＡＳＰ１ａとの時刻のずれによる影響を受けないで済むことになる。

【０１６５】

次いで、外部ＡＳＰ１ａは、通信ナビ５に対してサービスを開始し、通信ナビ５に地図データなどの種々のコンテンツを提供する（ステップＳ１８９，Ｓ１９０）。そして、外部ＡＳＰ１ａでは、ステップＳ１９１で通信ナビ５に送信すべきコンテンツの送信が完了したか否かを判断する。つまり、ステップＳ１９１ではＤＬＬが完了したか否かを判断し、完了しない場合（ステップＳ１９１；ＮＯ）には、ステップＳ１９２でセッションキーの有効時間を確認した後、上述したステップＳ１７７の認証処理に戻る。また、コンテンツの送信が完了した場合（ステップＳ１９１；ＹＥＳ）には、外部ＡＳＰ１ａの全体の処理を終了する。

【０１６６】

一方、通信ナビ５は、ステップＳ１９３で受信すべき全てのコンテンツの受信が完了したか否かを判断し、コンテンツの受信が完了するまで外部ＡＳＰ１ａと送受信処理（ステップＳ１９０）を実行し、コンテンツの受信が完了した場合（（ステップＳ１９３；ＹＥＳ）には、通信ナビ５の全体の処理を終了する。

【０１６７】

なお、本実施形態では、外部ＡＳＰ１ａがインターネットＩＮを介してサーバ装置１および通信端末装置２に対して送受信可能としたが、これに限らず専用回線を介して送受信可能としてもよい。

【０１６８】

このように本実施形態によれば、サーバ装置１により生成されたセッションキーを認証する認証共通部１２ａを、サーバ装置１とは外部ＡＳＰ１ａに設けたこ

とにより、サーバ装置１のＣＰＵ容量を低減させることができる。

【０１６９】

また、本実施形態によれば、外部ＡＳＰ１ａは、セッションキーを取得した時刻とアクセス許可残り時間に基づいて地図データなどのデータに対してアクセスする時間を設定することにより、外部ＡＳＰ１ａを用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【０１７０】

なお、上述した各実施形態では、車両に搭載された通信端末装置２の通信ナビ５を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置１から通信ナビ５に地図データなどのデータを供給する通信機器認証システムに対して本発明を適用した例について説明したが、これに限らずパソコン３や携帯電話機４などのように他の通信端末装置に対して認証を行い、その認証結果に基づいてサーバ装置１から各種データを供給する通信機器認証システムに対しても適用可能である。

【０１７１】

また、上記各実施形態では、通信手段としてインターネットＩＮを用いたが、これに限らず専用回線または公衆回線などを用いた通信ネットワークを使用してもよい。

【０１７２】

さらに、上記各実施形態では、通信端末装置としてパソコン３、携帯電話機４および通信ナビ５を用いたが、これに限らず通信機能付きの各種モバイル端末、あるいは通信機能付きの家電製品などであってもよい。

【０１７３】

そして、上記図１４および図１６を除く図６～図１７に示したフローチャートに対するプログラムを、フレキシブルディスクまたはハードディスクなどの情報記録媒体に記録させておき、これを汎用のマイクロコンピュータなどに読み出して実行させることで、そのマイクロコンピュータを上記実施形態におけるサーバ装置１または外部ＡＳＰ１ａとして機能させることが可能である。

【０１７４】

【発明の効果】

以上説明したように本発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１７５】

請求項２に記載の発明によれば、請求項１に記載の効果に加えて、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０１７６】

請求項３に記載の発明によれば、請求項１または２に記載の効果に加えて、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【０１７７】

請求項４に記載の発明によれば、請求項１に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別

情報も受信することで、セキュリティを一段と高めることができる。

【０１７８】

請求項５に記載の発明によれば、請求項１に記載の効果に加えて、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【０１７９】

請求項６に記載の発明によれば、請求項１または５に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【０１８０】

請求項７に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証工程と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証工程と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１８１】

請求項８に記載の発明によれば、請求項７に記載の効果に加えて、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０１８２】

請求項９に記載の発明によれば、請求項７または８に記載の効果に加えて、第１の認証工程は、同一ユーザから別の通信端末装置を用いてユーザ特定情報が送

信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【０１８３】

請求項１０に記載の発明によれば、請求項７に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【０１８４】

請求項１１に記載の発明によれば、請求項７に記載の効果に加えて、第２のキー情報を認証する第３の認証工程を別のサーバ装置にて実行することにより、サーバ装置のＣＰＵ容量を低減させることができる。

【０１８５】

請求項１２に記載の発明によれば、請求項７または１１に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【０１８６】

請求項１３に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成して通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１８７】

請求項１４に記載の発明によれば、請求項１３に記載の効果に加えて、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０１８８】

請求項１５に記載の発明によれば、請求項１３または１４に記載の効果に加えて、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【０１８９】

請求項１６に記載の発明によれば、請求項１３に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【０１９０】

請求項１７に記載の発明によれば、請求項１３に記載の効果に加えて、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【０１９１】

請求項１８に記載の発明によれば、請求項１３または１７に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【０１９２】

請求項１９に記載の発明によれば、コンピュータを、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置から通信端末装置に送信する第１の認証手段、通信端末装置

から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置から通信端末装置に送信する第２の認証手段、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１９３】

請求項２０に記載の発明によれば、請求項１９に記載の効果に加えて、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０１９４】

請求項２１に記載の発明によれば、請求項１９または２０に記載の効果に加えて、第１の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【０１９５】

請求項２２に記載の発明によれば、請求項１９に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【０１９６】

請求項２３に記載の発明によれば、請求項１９に記載の効果に加えて、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サー

バ装置のＣＰＵ容量を低減させることができる。

【０１９７】

請求項２４に記載の発明によれば、請求項１９または２３に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【０１９８】

請求項２５に記載の発明によれば、請求項１９に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成して通信端末装置に送信する第１の認証手段と、通信端末装置から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成して通信端末装置に送信する第２の認証手段と、通信端末装置からサーバ装置への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第２のキー情報に有効時間を設けたことで、ＳＳＬを使用しない環境下での認証の際、パスワードの使用を極力削減し、ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【０１９９】

請求項２０に記載の通信機器認証用プログラムが記録されている場合には、第１のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第２のキー情報がデータに対してアクセスするセッションキーであることにより、ＳＳＬを使用しない認証の際、パスワードの代替とすることができる。

【０２００】

請求項２１に記載の通信機器認証用プログラムが記録されている場合には、第１の認証手段は、同一ユーザから別の通信端末装置を用いてユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を

用いることができる。

【０２０１】

請求項２２に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【０２０２】

請求項２３に記載の通信機器認証用プログラムが記録されている場合には、第２のキー情報を認証する第３の認証手段を別のサーバ装置に設けたことにより、サーバ装置のＣＰＵ容量を低減させることができる。

【０２０３】

請求項２４に記載の通信機器認証用プログラムが記録されている場合には、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【図面の簡単な説明】

【図１】

本発明に係る通信機器認証システムの第１実施形態の構成を示すブロック図である。

【図２】

図１のサーバ装置におけるデータベース部のデータ構造を示す説明図である。

【図３】

図２のデータ項目を示す説明図である。

【図４】

図１の通信端末装置であるパソコン、携帯電話機または通信カーナビゲーション装置の構成を示すブロック図である。

【図５】

図４のメモリ部に格納されるデータ構造を示す説明図である。

【図６】

第１実施形態の通信機器認証システムにおいて実行される通信ナビ接続までの

処理の概要を示すフローチャートである。

【図７】

図６のステップＳ１の詳細を示し、ユーザ登録（申込み番号付与）処理を実行するためのフローチャートである。

【図８】

図６のステップＳ２の詳細を示し、ユーザ登録（ユーザアカウント付与）処理を実行するためのフローチャートである。

【図９】

図６のステップＳ３の詳細を示し、簡易サインアップ処理を実行するためのフローチャートである。

【図１０】

図６のステップＳ４の詳細を示し、セッションキー取得処理を実行するためのフローチャートである。

【図１１】

図６のステップＳ５，Ｓ６の詳細を示し、通常アクセス認証処理を実行するためのフローチャートである。

【図１２】

本発明に係る通信機器認証システムの第２実施形態における通信端末追加処理を示すフローチャートである。

【図１３】

本発明に係る通信機器認証システムの第２実施形態における通信端末追加処理を示すフローチャートである。

【図１４】

（Ａ）は第２実施形態において単一アクセスキー使用時のデータ構造を示す説明図，（Ｂ）は第２実施形態において１アクセスキーを複数の通信端末装置で使用する場合のデータ構造を示す説明図である。

【図１５】

本発明に係る通信機器認証システムの第３実施形態における簡易サインアップ処理を示すフローチャートである。

【図１６】

本発明に係る通信機器認証システムの第４実施形態の構成を示すブロック図である。

【図１７】

第４実施形態の処理を示すフローチャートである。

【符号の説明】

１　サーバ装置（通信サービス系サーバ装置）

１ａ　外部ＡＳＰ（別のサーバ装置）

２　通信端末装置

３　パソコン

４　携帯電話機

５　通信カーナビゲーション装置

１１　通信回線送受信部

１２　認証共通部（第１の認証手段，第２の認証手段）

１２ａ　認証共通部（第３の認証手段）

１３　システム制御装置（アクセス許可手段）

１３ａ　システム制御装置

１４　アプリケーション部

１４ａ　アプリケーション部

１５　データベース部

１５ａ　データベース部

１６　通信回線送受信部

１７　システム制御部

１８　操作部

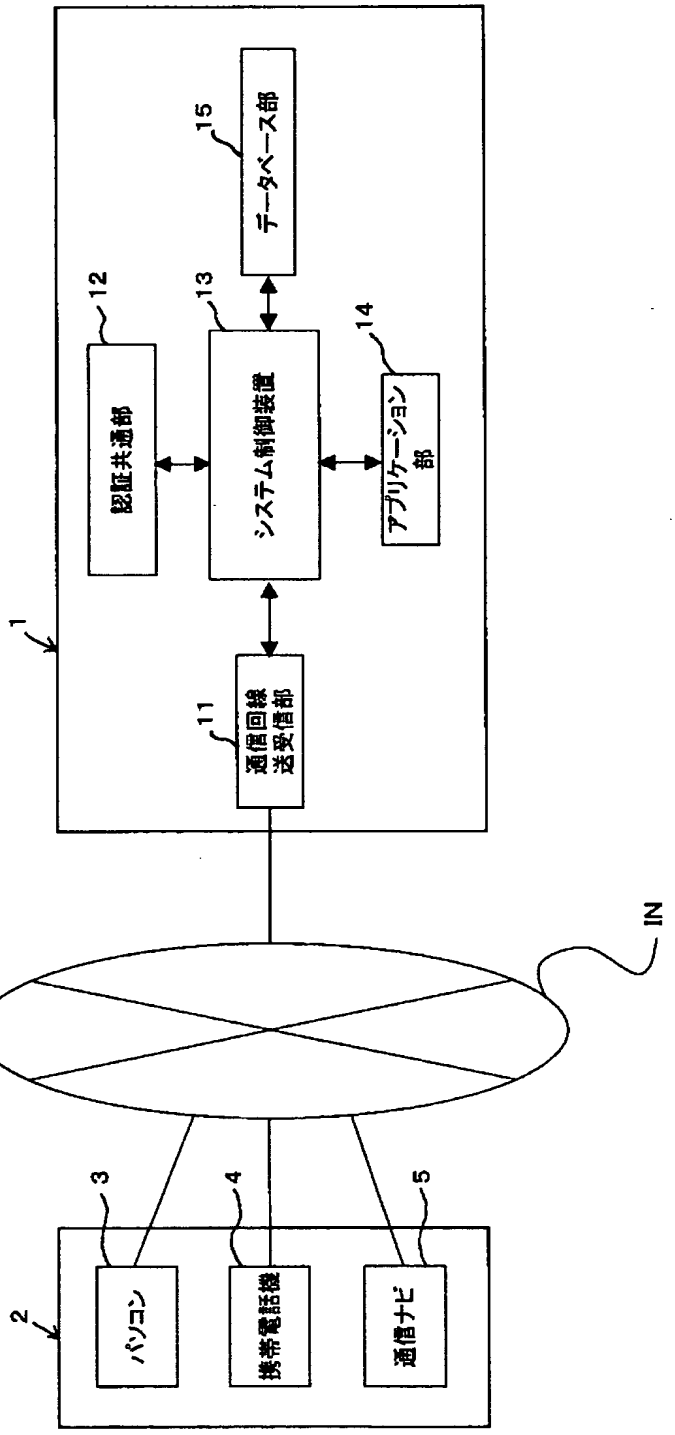
１９　表示部

２０　メモリ部

ＩＮ　インターネット（通信手段）

【書類名】　　図面

【図１】


1
2
3
4
5
11
12
13
14
15
IN
認証共通部
システム制御装置
アプリケーション部
データベース部
通信回線送受信部
パソコン
携帯電話機
通信ナビ

【図２】

氏名	住所	電話　号	メールアドレス	申込みNo	クレジットカードNo
通信　太郎	東京都目黒区○○	03-1234-1234	mft@ipc.co.jp	200204091405	1234-1234-1234-1234
認証　太郎	東京都葛飾区○○	03-1233-1233	nst@ipc.co.jp	200204091406	2222-2222-2222-2222

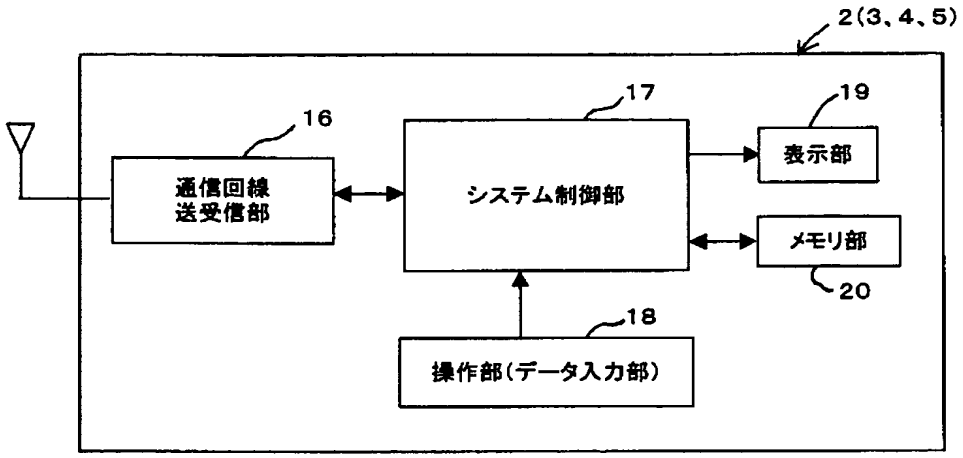
クレジットカード有効期限	ユーザID	パスワード	ライセンス番号	アクセスキー	メーカID
06-03	123123	456456	23217	ack0101	56789
06-03	123456	456789	22231	ack5555	56789

型番ID	ハードウェアNo	セッションキー	セッションキー有効時間
20345687	568977	ssk0023	1705
20345687	348977	ssk0056	1510

【図３】

データ登録項目	ユーザ登録時必要項目	簡易サインアップ通常アクセス時必要項目	サーバ装置データ登録	通信ナビデータ登録
氏名	○		○	
住所	○		○	
電話番号	○		○	
メールアドレス	○		○	
申込みNo	○		○	
クレジットカードNo	○		○	
クレジットカード有効期限	○		○	
ユーザID	○	○	○	○
パスワード	○	○	○	
ライセンス番号	○	○	○	○
アクセスキー		○	○	○
メーカID		○	○	
型番ID		○	○	
ハードウェアNo		○	○	
セッションキー		○	○	○
セッションキー有効時間		○	○	

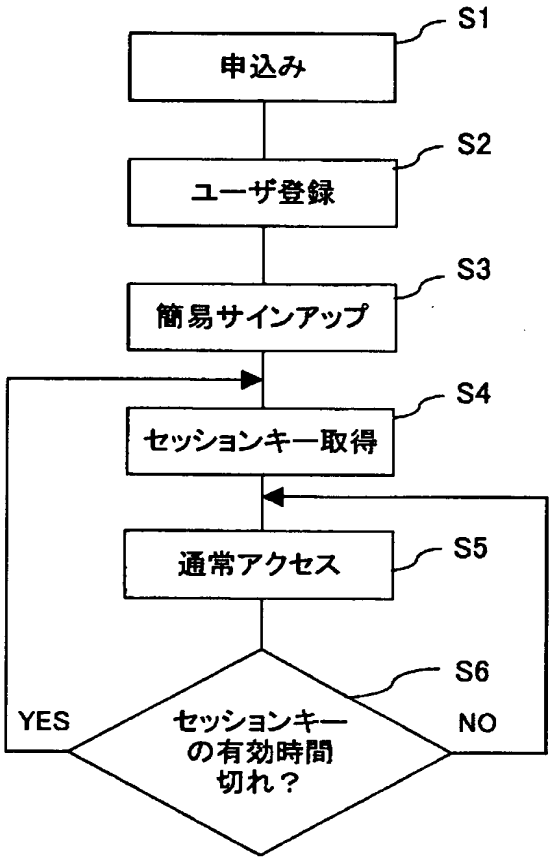
【図４】



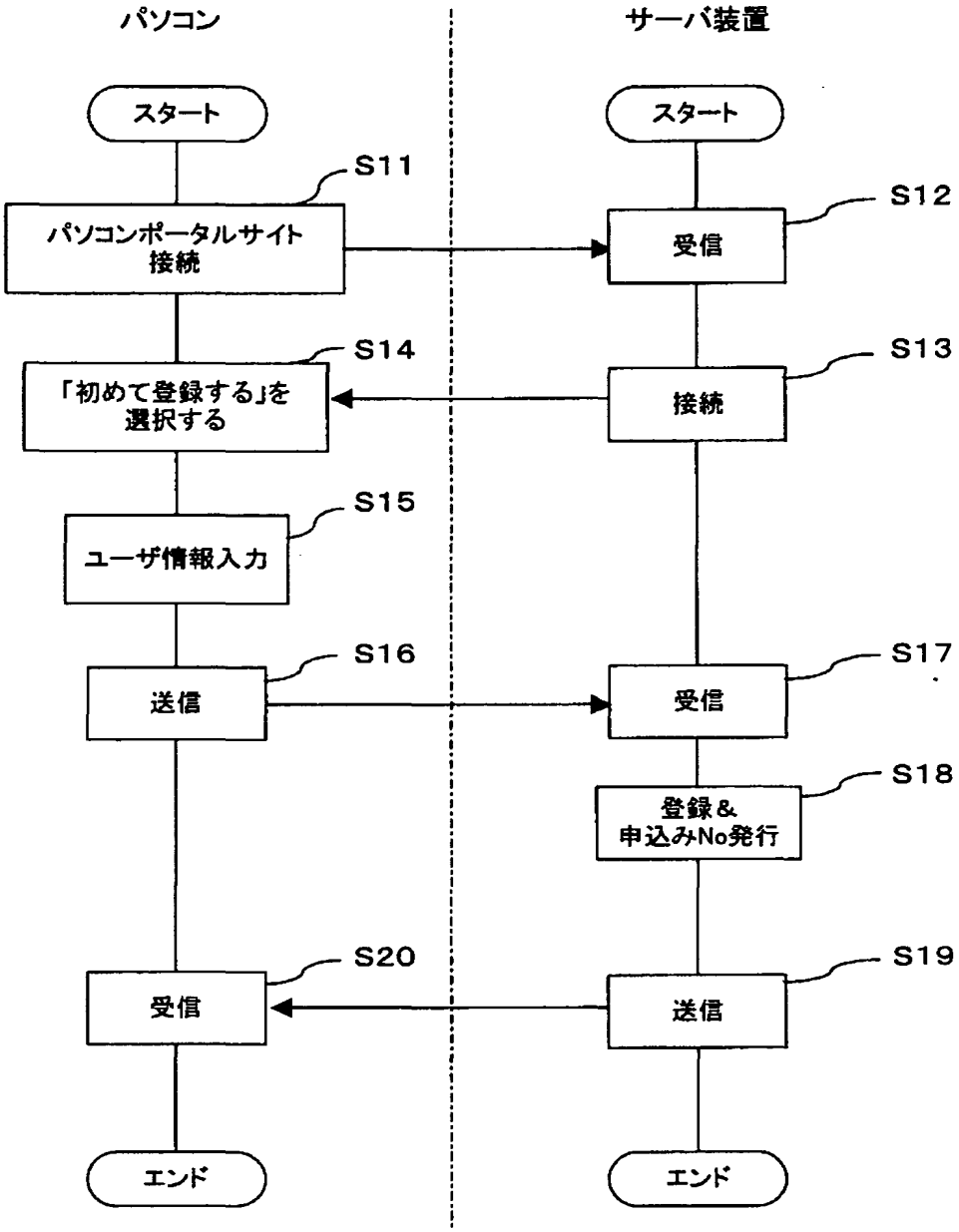
【図５】

ユーザID	ライセンス番号	アクセスキー	セッションキー
123123	23217	ack0101	ssk0023

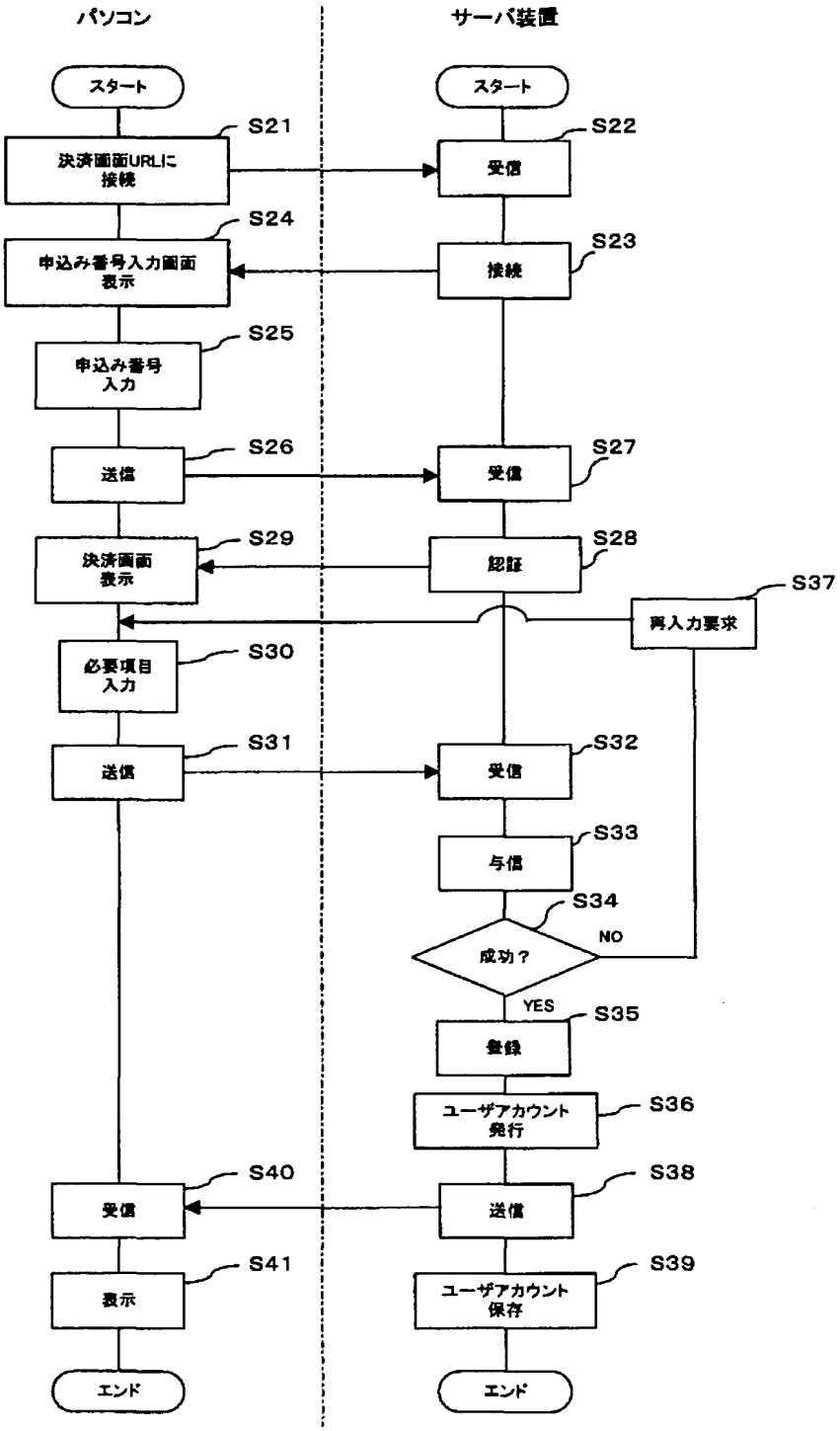
【図６】


S1
申込み
S2
ユーザ登録
S3
簡易サインアップ
S4
セッションキー取得
S5
通常アクセス
S6
セッションキーの有効時間切れ？
YES
NO

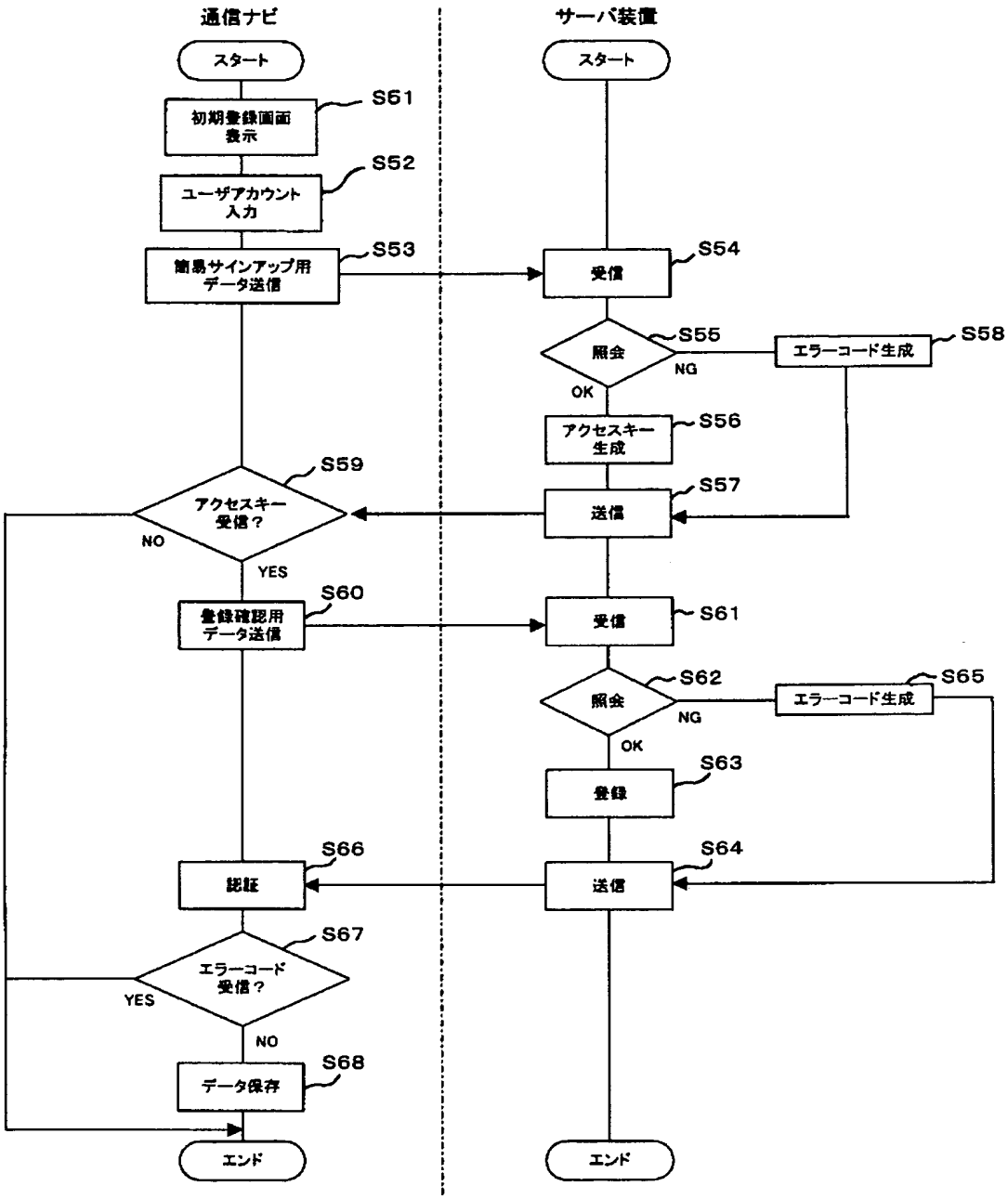
【図７】


パソコン
サーバ装置
スタート
スタート
S11
パソコンポータルサイト
接続
S12
受信
S14
「初めて登録する」を
選択する
S13
接続
S15
ユーザ情報入力
S16
送信
S17
受信
S18
登録＆
申込みNo発行
S20
受信
S19
送信
エンド
エンド

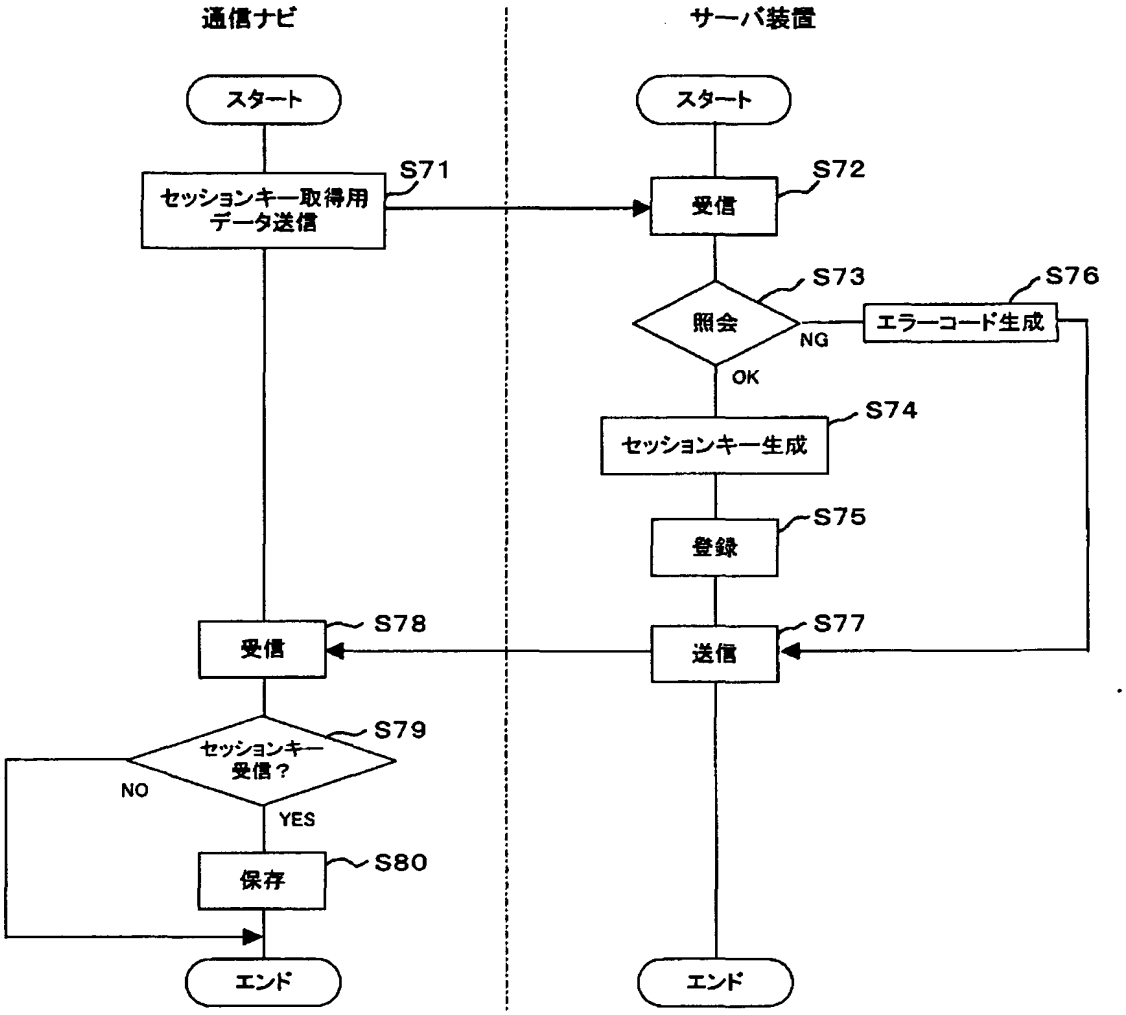
【図８】


パソコン
サーバ装置
スタート
スタート
S21
決済画面URLに接続
S22
受信
S24
申込み番号入力画面表示
S23
接続
S25
申込み番号入力
S26
送信
S27
受信
S29
決済画面表示
S28
認証
S37
再入力要求
S30
必要項目入力
S31
送信
S32
受信
S33
与信
S34
成功？
NO
YES
S35
登録
S36
ユーザアカウント発行
S40
受信
S38
送信
S41
表示
S39
ユーザアカウント保存
エンド
エンド

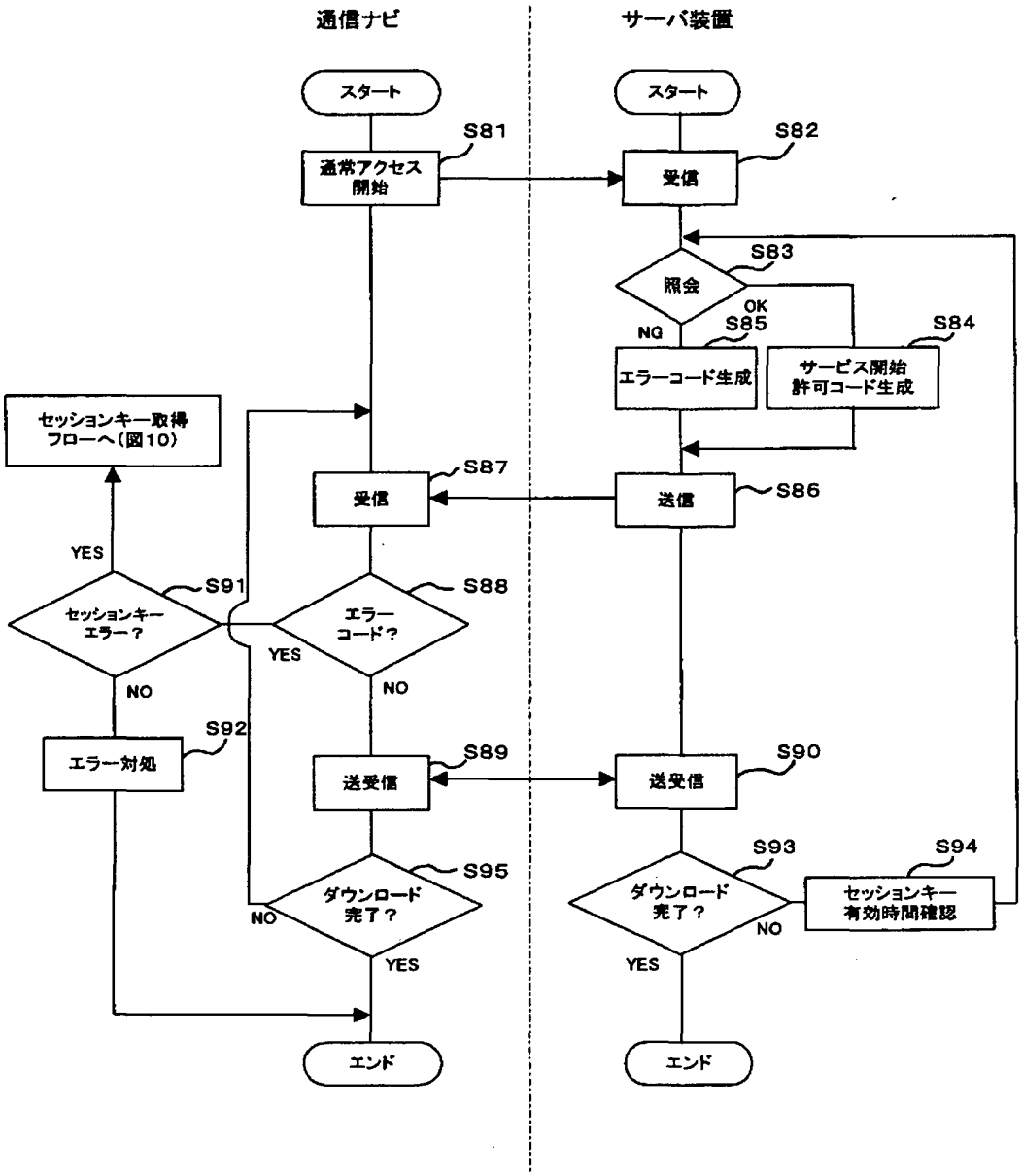
【図９】


通信ナビ
サーバ装置
スタート
スタート
初期登録画面表示
S61
ユーザアカウント入力
S52
簡易サインアップ用データ送信
S53
受信
S54
照会
S55
NG
エラーコード生成
S58
OK
アクセスキー生成
S56
送信
S57
アクセスキー受信？
S59
NO
YES
登録確認用データ送信
S60
受信
S61
照会
S62
NG
エラーコード生成
S65
OK
登録
S63
認証
S66
送信
S64
エラーコード受信？
S67
YES
NO
データ保存
S68
エンド
エンド

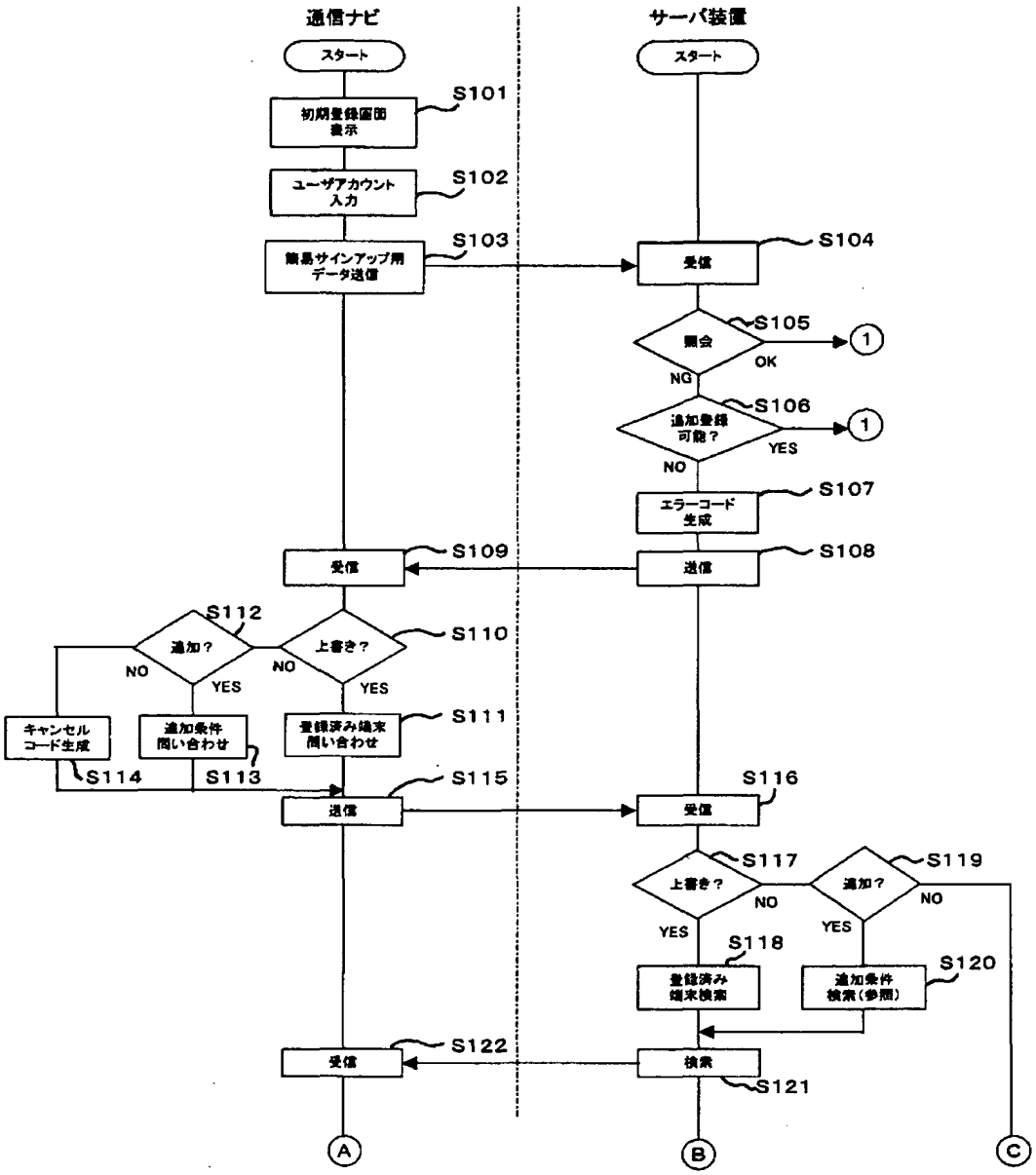
【図１０】


通信ナビ
サーバ装置
スタート
スタート
S71
セッションキー取得用データ送信
S72
受信
S73
照会
S76
エラーコード生成
NG
OK
S74
セッションキー生成
S75
登録
S78
受信
S77
送信
S79
セッションキー受信？
NO
YES
S80
保存
エンド
エンド

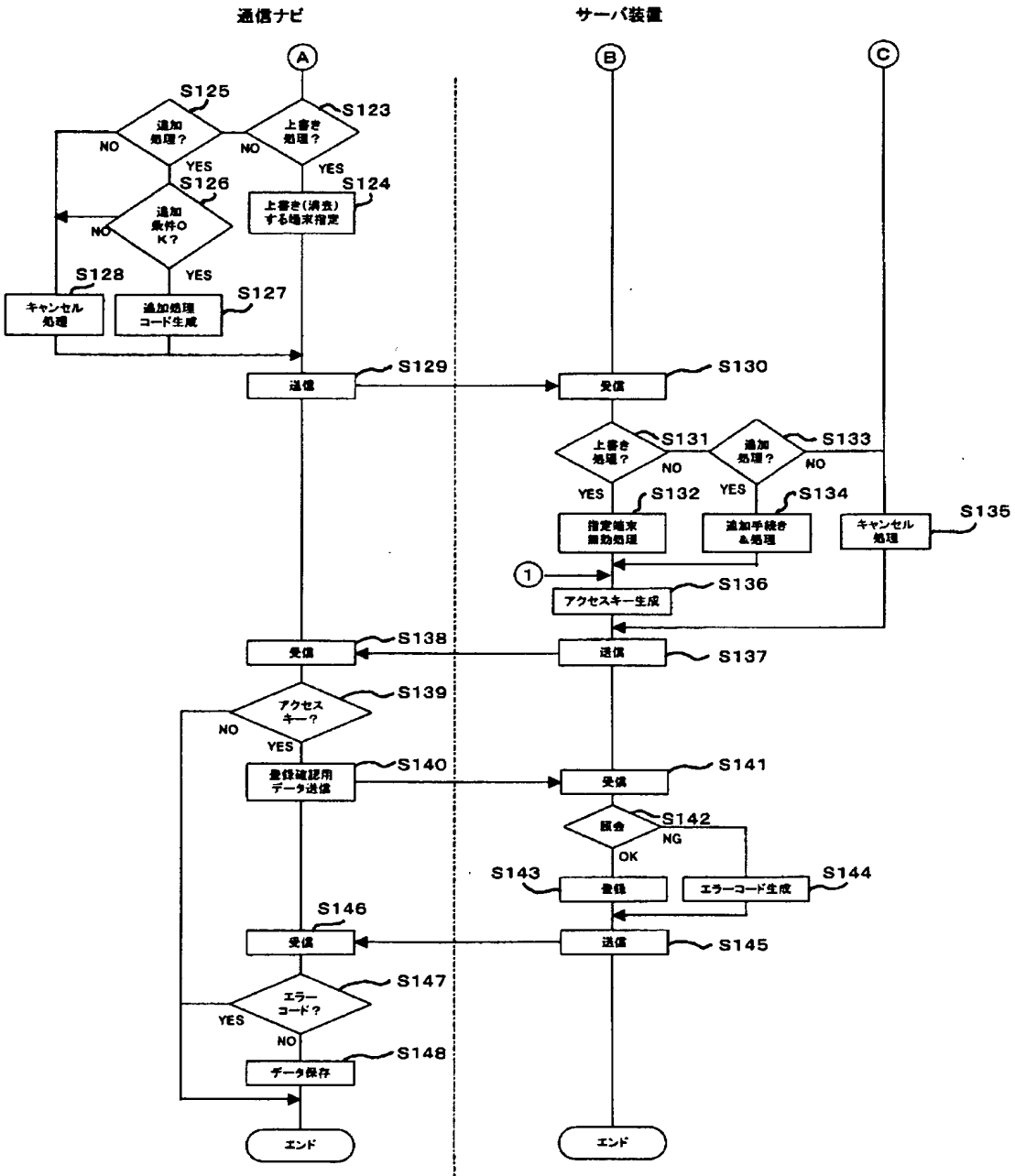
【図１１】


通信ナビ
サーバ装置
スタート
スタート
S81
通常アクセス開始
S82
受信
S83
照会
OK
NG
S85
エラーコード生成
S84
サービス開始許可コード生成
セッションキー取得フローへ(図10)
S87
受信
送信
S86
YES
S91
セッションキーエラー？
S88
エラーコード？
YES
NO
NO
S92
エラー対処
S89
送受信
送受信
S90
S95
ダウンロード完了？
NO
YES
S93
ダウンロード完了？
NO
S94
セッションキー有効時間確認
YES
エンド
エンド

【図１２】


通信ナビ
サーバ装置
スタート
スタート
S101
初期登録画面表示
S102
ユーザアカウント入力
S103
簡易サインアップ用データ送信
S104
受信
S105
照会
OK
NG
1
S106
追加登録可能？
YES
NO
1
S107
エラーコード生成
S108
送信
S109
受信
S110
上書き？
NO
YES
S112
追加？
NO
YES
S111
登録済み端末問い合わせ
追加条件問い合わせ
キャンセルコード生成
S113
S114
S115
送信
S116
受信
S117
上書き？
NO
YES
S119
追加？
NO
YES
S118
登録済み端末検索
S120
追加条件検索（参照）
S121
検索
S122
受信
A
B
C

【図１３】


通信ナビ
サーバ装置
A
B
C
S125
追加処理？
NO
YES
S123
上書き処理？
NO
YES
S126
追加条件OK？
NO
YES
S124
上書き(消去)する端末指定
S128
キャンセル処理
S127
追加処理コード生成
S129
送信
S130
受信
S131
上書き処理？
NO
YES
S133
追加処理？
NO
YES
S132
指定端末削除処理
S134
追加手続き&処理
S135
キャンセル処理
①
S136
アクセスキー生成
S138
受信
S137
送信
S139
アクセスキー？
NO
YES
S140
登録確認用データ送信
S141
受信
S142
照合
NG
OK
S143
登録
S144
エラーコード生成
S146
受信
S145
送信
S147
エラーコード？
YES
NO
S148
データ保存
エンド
エンド

【図１４】

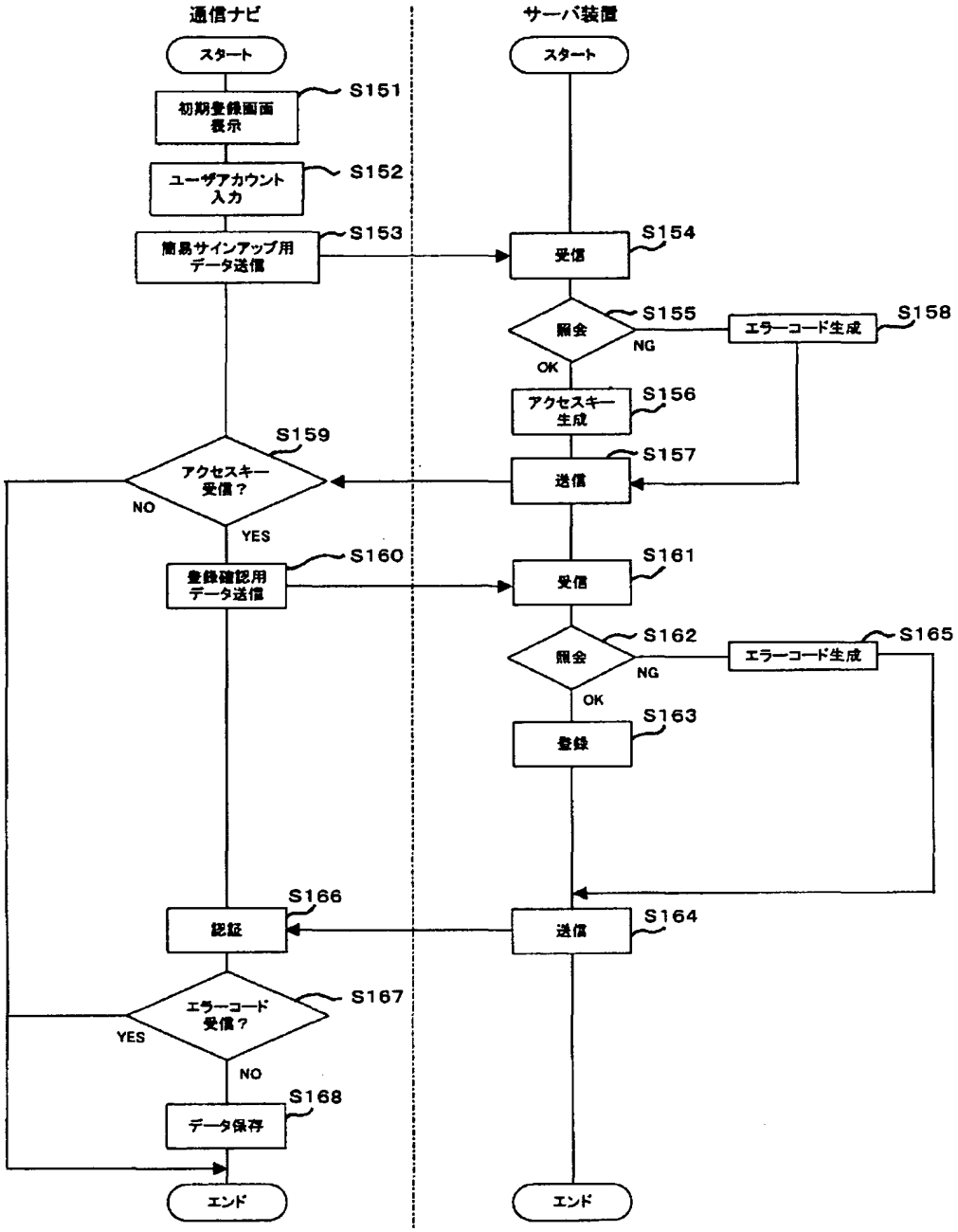
(A)

ユーザID	パスワード	アクセスキー	メーカID	型番ID
00001	0101	ack01	P01	Y01-0001
00001	0101	ack02	P01	Y02-1234
⋮	⋮	⋮	⋮	⋮

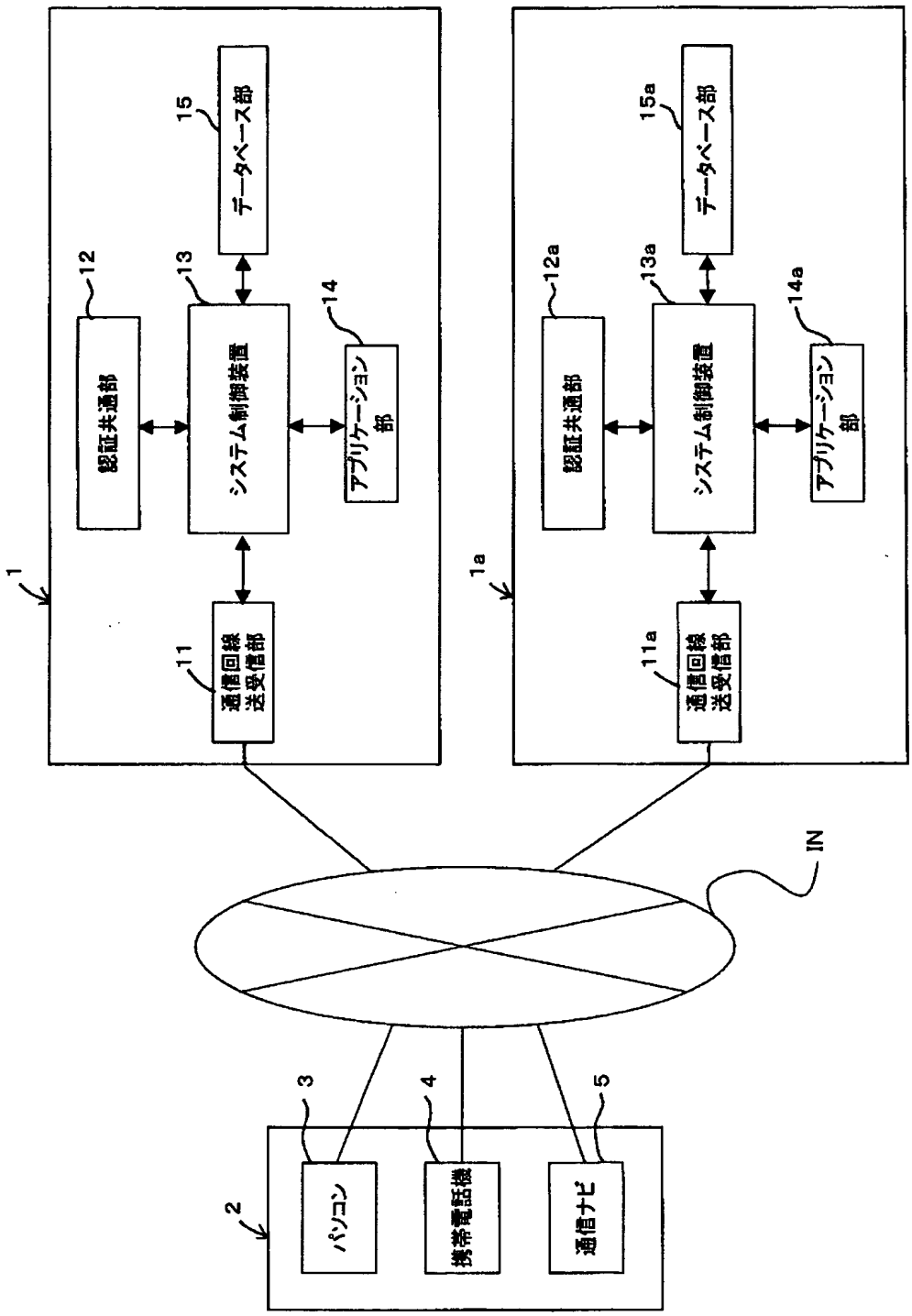
(B)

ユーザID	パスワード	アクセスキー	メーカID	型番ID
00001	0101	ack01	P01	Y01-0001
00001	0101	ack01	P01	Y02-1234
⋮	⋮	⋮	⋮	⋮

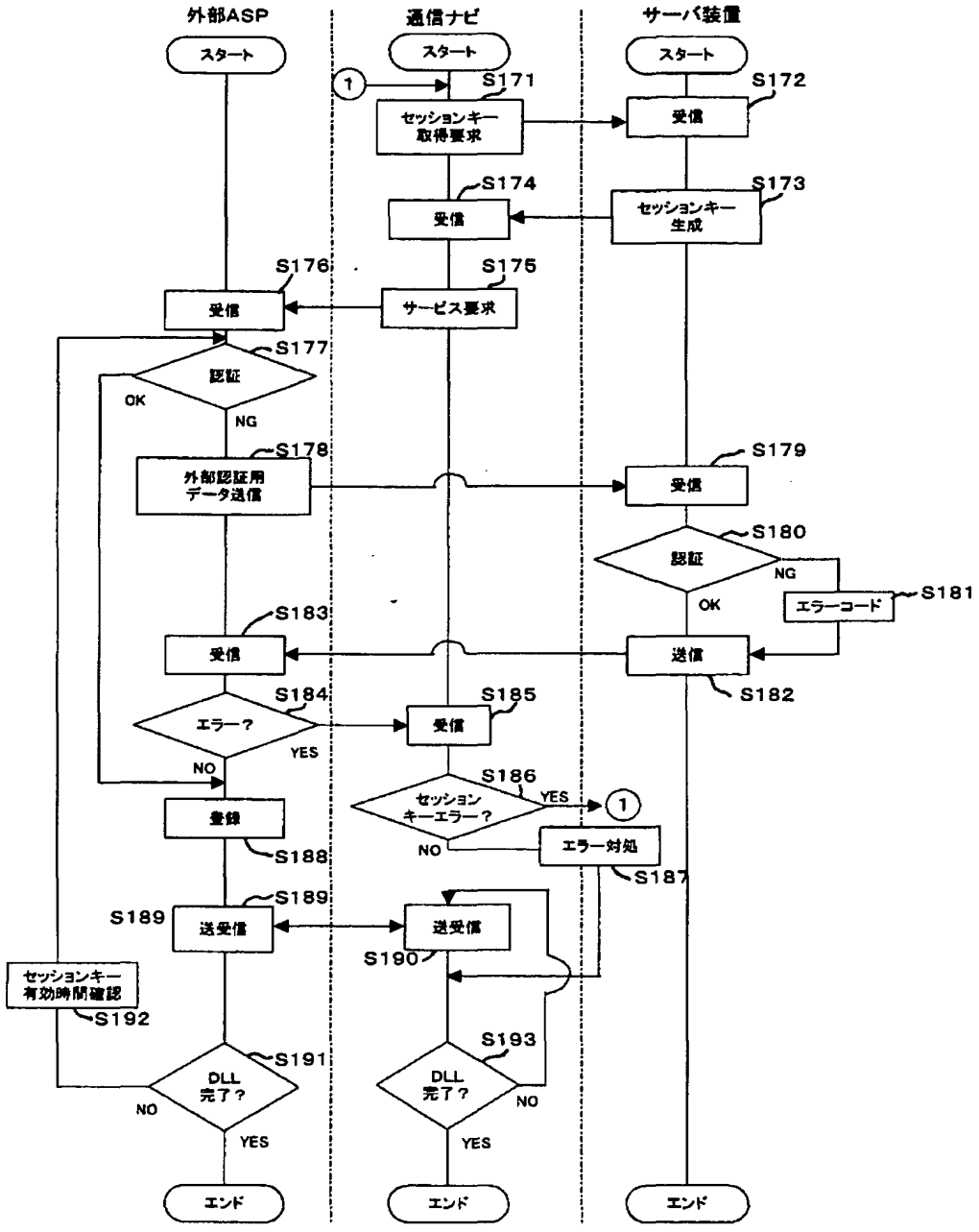
【図１５】


通信ナビ
サーバ装置
スタート
スタート
初期登録画面表示
S151
ユーザアカウント入力
S152
簡易サインアップ用データ送信
S153
受信
S154
照会
S155
NG
エラーコード生成
S158
OK
アクセスキー生成
S156
送信
S157
アクセスキー受信？
S159
NO
YES
登録確認用データ送信
S160
受信
S161
照会
S162
NG
エラーコード生成
S165
OK
登録
S163
認証
S166
送信
S164
エラーコード受信？
S167
YES
NO
データ保存
S168
エンド
エンド

【図１６】


1
認証共通部
12
システム制御装置
13
データベース部
15
アプリケーション部
14
通信回線送受信部
11
1a
認証共通部
12a
システム制御装置
13a
データベース部
15a
アプリケーション部
14a
通信回線送受信部
11a
IN
2
パソコン
3
携帯電話機
4
通信ナビ
5

【図１７】


外部ASP
通信ナビ
サーバ装置
スタート
スタート
スタート
1
S171
セッションキー取得要求
S172
受信
S174
受信
S173
セッションキー生成
S176
受信
S175
サービス要求
S177
認証
OK
NG
S178
外部認証用データ送信
S179
受信
S180
認証
NG
OK
エラーコード
S181
S183
受信
送信
S182
S184
エラー？
YES
NO
S185
受信
S186
セッションキーエラー？
YES
NO
1
エラー対処
S187
登録
S188
S189
S189
送受信
送受信
S190
セッションキー有効時間確認
S192
S191
DLL完了？
NO
YES
S193
DLL完了？
NO
YES
エンド
エンド
エンド

【書類名】　　要約書

【要約】

【課題】ＣＰＵの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、不正アクセスを防止し、セキュリティを著しく向上させる。

【解決手段】通信端末装置２から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第１のキー情報を生成してサーバ装置１から通信端末装置２に送信する第１の認証手段１２と、通信端末装置２から送信される第１のキー情報を認証し、当該第１のキー情報に基づいてデータに対してアクセスする第２のキー情報を生成してサーバ装置１から通信端末装置２に送信する第２の認証手段１２と、通信端末装置２からサーバ装置１への第２のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段１３とを備えた。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔５９５１０５５１５〕

１．変更年月日　　１９９５年　７月２１日
［変更理由］　新規登録
住　所　東京都目黒区下目黒１丁目７番１号
氏　名　インクリメント・ピー株式会社